CNIL 2026 : du gendarme RGPD au régulateur de l'IA

Le 7 avril 2026, la CNIL publie son programme de travail annuel et y inscrit une phrase qui passe presque inaperçue : l'autorité « se prépare à être désignée autorité de surveillance de marché au titre du règlement européen sur l'intelligence artificielle, en plus de ses fonctions d'autorité de protection des droits fondamentaux ». Derrière l'apparente continuité administrative, c'est un changement d'instrument d'action publique qui s'opère. Pour le SI public, la question n'est plus de savoir si la CNIL aura compétence sur les systèmes d'IA à haut risque déployés en France. Elle est de savoir quel instrument l'autorité mobilisera, et avec quels effets sur la régulation effective des projets en cours.

Par Alexandre Berge · 24 mai 2026 · 18 min de lecture · Analyse

Un programme annuel qui acte une mue institutionnelle

Le document publié début avril 2026 sur cnil.fr structure six axes de travail (consentement, intelligence artificielle, logement social, données de santé, droit d'accès, cybersécurité). Lu rapidement, il ressemble à n'importe quel programme annuel d'autorité administrative indépendante. Lu attentivement, il acte un repositionnement.

Trois éléments le signalent. D'abord la finalisation, annoncée pour 2026, des fiches sectorielles « IA au travail » et « IA en santé », cette dernière co-publiée avec la Haute Autorité de santé après une consultation publique close le 16 avril 2026. Ensuite l'ouverture d'un chantier doctrinal majeur sur « l'application du RGPD aux modèles non anonymes », qui prolonge l'avis 28/2024 du Comité européen de la protection des données et étend la portée du règlement général au-delà de la seule phase d'entraînement, vers la phase de déploiement et de réutilisation des modèles. Enfin la formulation explicite de la préparation à un nouveau rôle institutionnel, formulation rare dans un programme annuel et qui vaut acte de prise de date sur le 2 août 2026, échéance d'entrée en application des obligations « haut risque » de l'AI Act.

Cette bascule s'inscrit dans une séquence plus large. Le 22 juillet 2025, la CNIL avait finalisé ses recommandations sur le développement des systèmes d'IA, treize fiches couvrant le cycle de vie complet, de la qualification juridique à la sécurité, en passant par le moissonnage et l'annotation. Le 3 avril 2026, elle annonce ses contrôles thématiques prioritaires (recrutement, Répertoire électoral unique, fédérations sportives) et présente explicitement la

thématique « recrutement » comme préfigurant son futur rôle d'autorité de surveillance du marché dans le champ « travail » au titre de l'AI Act. Le 9 février 2026, son bilan annuel des sanctions affichait 83 décisions et 486 839 500 euros d'amendes prononcées en 2025, dont une amende de 5 millions d'euros infligée à France Travail le 22 janvier 2026 pour défaut de sécurité après l'exfiltration de données concernant 36,8 millions de personnes. Le message politique est clair : l'autorité monte en puissance sanctionnatrice sur le secteur public juste avant d'élargir son périmètre.

Ce que le mot « surveillance » veut dire

L'angle mort du débat public sur cette bascule réside dans un mot que les commentateurs traitent comme un synonyme et qui n'en est pas un : « surveillance ». La CNIL exerce depuis 1978 une surveillance des traitements de données. Elle exercera demain une surveillance de marché des systèmes d'IA. Les deux mots se ressemblent. Les deux instruments ne se ressemblent pas.

Pierre Lascoumes et Patrick Le Galès, dans *Gouverner par les instruments* (Presses de Sciences Po, 2004), proposent la grille analytique qui permet de nommer ce qui se joue. Un instrument d'action publique est selon eux « un dispositif à la fois technique et social qui organise des rapports sociaux spécifiques entre la puissance publique et ses destinataires en fonction des représentations et des significations dont il est porteur ». Toute technique retenue, soulignent-ils, est « créatrice d'effets propres qui débordent les effets attendus ». Le choix d'un instrument plutôt que d'un autre n'est jamais neutre : il définit qui parle au nom de quel intérêt, sur quels critères, avec quels effets de cadrage du problème lui-même.

> **L'instrumentation de l'action publique chez Lascoumes et Le Galès**
>
> Dans *Gouverner par les instruments* (Presses de Sciences Po, 2004), Pierre Lascoumes et Patrick Le Galès définissent un instrument d'action publique comme « un dispositif à la fois technique et social qui organise des rapports sociaux spécifiques entre la puissance publique et ses destinataires en fonction des représentations et des significations dont il est porteur ». Ils distinguent quatre grands types d'instruments (législatif et réglementaire, économique et fiscal, conventionnel et incitatif, informatif et communicationnel), auxquels s'ajoutent les normes, standards et bonnes pratiques. À chacun correspond une légitimité propre et un rapport politique distinct (l'État tuteur du social pour le réglementaire, l'État mobilisateur pour l'incitatif, la démocratie du public pour l'informationnel, les ajustements concurrentiels pour les standards). La thèse centrale est que tout choix d'instrument est une décision politique, jamais une simple décision technique.

Appliquée à la CNIL, cette grille révèle trois moments. Premier moment, 1978. La loi Informatique et Libertés du 6 janvier 1978 crée une autorité administrative indépendante (la première de ce nom dans le droit français) en réaction à l'émoi suscité par le projet SAFARI de

1974. L'instrument est garantiste, fondé sur la légitimité d'un tiers institutionnel chargé de protéger un droit fondamental nouveau, la vie privée informationnelle. Capacités réglementaires limitées (recommandations, délibérations), forte capacité informationnelle (publication, pédagogie, normalisation par la doctrine). Le rapport politique est celui d'un État tuteur des droits face à l'informatique de gestion.

Deuxième moment, mai 2018. L'entrée en application du règlement général sur la protection des données bascule l'autorité d'un régime déclaratif vers un régime de redevabilité, et la dote d'un instrument sanctionnateur d'une intensité inédite. Les amendes deviennent un levier de cadrage des pratiques. Le rapport politique change : la CNIL ne tutelle plus seulement, elle sanctionne et oriente par le risque financier. Mais l'objet reste celui de 1978 : la donnée personnelle, traitée selon une logique de plainte, de droit subjectif, de responsable de traitement identifié.

Troisième moment, 2026. L'AI Act ne réforme pas le RGPD, il s'y superpose. Or sa logique n'est pas celle des droits fondamentaux, c'est celle de la **surveillance du marché des produits**. Le règlement (UE) 2024/1689 hérite directement, dans son architecture, du règlement (UE) 2019/1020 sur la surveillance du marché des produits manufacturés. Il introduit dans le périmètre CNIL des objets étrangers à sa culture : la conformité de produit, l'évaluation par des organismes notifiés, la base européenne des systèmes d'IA à haut risque, la coopération avec les autorités douanières, les obligations d'information pesant sur les fournisseurs avant la mise sur le marché. La logique est objective (le produit conforme ou non), descendante (l'enquête d'office), industrielle (les fabricants et les déployeurs comme destinataires). La logique RGPD, elle, est subjective (la personne concernée), ascendante (la plainte), administrative (le responsable de traitement comme destinataire principal).

La bascule par l'instrument est donc plus profonde que la simple extension d'une compétence. C'est l'arrivée, dans une autorité construite autour d'un instrument garantiste, d'un instrument hérité du droit de la consommation et de la libre circulation des marchandises. La question n'est pas de savoir si la CNIL peut techniquement endosser ce rôle. La question est de savoir si l'instrument « surveillance de marché » va recoloniser, dans la pratique de l'autorité, l'instrument « droit fondamental », ou si la coexistence des deux produira une hybridation cohérente.

Une architecture française qui dilue la trajectoire

Le choix français de gouvernance amplifie cette incertitude. À la différence de l'Espagne, qui a créé dès 2023 une agence dédiée, l'Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), opérationnelle depuis février 2025 à La Corogne et dotée de la pleine puissance sanctionnatrice depuis le 2 août 2025, la France a opté pour une architecture éclatée.

Le projet présenté par la Direction générale des entreprises et la Direction générale de la

concurrence, de la consommation et de la répression des fraudes en septembre 2025 confiait la surveillance à une quinzaine d'autorités sectorielles, avec la DGCCRF comme coordinatrice et point de contact unique au sens de l'article 70 de l'AI Act. Or l'étude du Conseil d'État « Intelligence artificielle et action publique : construire la confiance, servir la performance » du 30 août 2022 avait recommandé exactement l'inverse : « une transformation profonde de la CNIL en autorité de contrôle nationale responsable de la régulation des systèmes d'IA, notamment publics ». La recommandation n'avait pas été suivie.

Un revirement partiel intervient en février 2026. Le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne, adopté en première lecture au Sénat le 17 février 2026, confie finalement à la CNIL la surveillance des cas d'usage à haut risque les plus régaliens. La rapporteure Marie-Lise Housseau présentait ainsi l'amendement n° 442 : il « tend à faire de la Cnil l'autorité de surveillance des systèmes d'IA à haut risque qui seront utilisés dans de nombreux domaines régaliens très sensibles en matière de droits et libertés fondamentaux : la biométrie, l'emploi, la répression, les contrôles aux frontières, ou encore les processus démocratiques ». Le sénateur Thomas Dossus, du groupe Écologiste, déplorait la même séance l'absence d'autorité unique dédiée et l'illisibilité d'un dispositif à quinze entités.

> **La carte française des autorités de surveillance AI Act (état au 17 février 2026)**
>
> Au terme du vote en première lecture au Sénat, la répartition retenue confie à la CNIL la surveillance des pratiques interdites (article 5) en duo avec la DGCCRF, la police prédictive, la biométrie, la reconnaissance d'émotions, la catégorisation biométrique, l'emploi (annexe III §4), les services publics et privés essentiels (§5, hors finance), la répression (§6), la migration et les frontières (§7), les processus démocratiques (§8b, en consultation obligatoire avec l'Arcom). L'ACPR garde les services financiers, l'ANSM les dispositifs médicaux, le Haut fonctionnaire de défense et de sécurité (Bercy et Transition écologique) les infrastructures critiques, le Conseil d'État, la Cour de cassation et la Cour des comptes la justice dans leur ordre juridictionnel. La DGCCRF est désignée point de contact unique au sens de l'article 70.2. L'ANSSI et le PEReN apportent un appui technique mutualisé. Le texte doit encore passer à l'Assemblée nationale et peut évoluer sous l'effet du paquet Digital Omnibus européen présenté en novembre 2025.

Le modèle français contraste avec les trois autres grands États membres. L'Italie, par la loi 132/2025 du 23 septembre 2025, a désigné AgID comme autorité de notification et l'Agenzia per la Cybersicurezza Nazionale comme autorité de surveillance et point de contact unique, en conservant les compétences sectorielles du Garante Privacy, de l'AGCOM, de la Banca d'Italia, de la CONSOB et de l'IVASS. L'Allemagne, par le projet KI-MIG approuvé en Conseil des ministres le 11 février 2026, fait de la Bundesnetzagentur l'autorité centrale, avec création d'une chambre indépendante interne pour les systèmes à haut risque les plus sensibles (police, migration, justice, démocratie) et rapport annuel au Bundestag. L'Espagne a fait le choix le plus radical de la centralisation dans une agence dédiée.

Le parallèle structurel le plus parlant n'est pourtant pas dans cette comparaison synchronique. Il est dans la propre histoire de la CNIL. En 2018, l'entrée en application du RGPD avait déjà élargi le périmètre de l'autorité et changé son instrumentation. Mais elle l'avait fait sans modifier sa matrice culturelle : la donnée personnelle restait l'objet, le responsable de traitement restait le destinataire, la plainte de la personne concernée restait le mode opératoire dominant. L'instrument sanctionnateur s'ajoutait à l'instrument informationnel sans le contredire. La bascule de 2026 est d'une autre nature. Elle introduit un objet (le système d'IA comme produit), un destinataire (le fournisseur, l'importateur, le distributeur, le déployeur) et un mode opératoire (l'enquête de conformité) qui obéissent à une autre grammaire administrative. Le précédent de 2018 ne préfigure donc pas 2026, il en marque les limites.

L'angle mort : l'absence de FRIA publics dans le SI public

C'est sur ce terrain que se loge l'angle mort le plus net du discours institutionnel. L'AI Act, à son article 27, oblige les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics, à conduire une analyse d'impact sur les droits fondamentaux (Fundamental Rights Impact Assessment, ou FRIA) avant le premier déploiement d'un système à haut risque. Le contenu attendu est explicite : description des processus, période et fréquence d'utilisation, catégories de personnes affectées, risques spécifiques, mesures de supervision humaine, mesures d'atténuation, gouvernance et plainte. L'article 27.5 prévoit que l'AI Office publiera un template officiel pour standardiser cette analyse.

L'écart entre cette obligation et l'état du terrain français au 22 mai 2026 est saisissant. Aucune analyse d'impact sur les droits fondamentaux rendue par un organisme public français n'est publique à cette date. Le template officiel de l'AI Office n'a pas été publié. Aucun guide CNIL ou DINUM autonome dédié au FRIA n'existe, à l'exception du guide commun Haute Autorité de santé et CNIL sur « l'IA en contexte de soins », publié en consultation entre février et avril 2026, qui mentionne explicitement « la réalisation d'une analyse d'impact sur les droits fondamentaux (AIDF) prévue à l'article 27 du RIA pour les déployeurs de droit public ou fournissant des services publics ».

Or les déploiements d'IA dans le SI public français qui entrent potentiellement dans le périmètre de l'annexe III ne manquent pas. France Travail a déployé en 2024 le « Conseils Personnalisés » (accompagné par le bac à sable CNIL), puis le Journal de la Recherche d'Emploi et le Chat FT (annexe III §4 sur l'emploi). La Direction générale des finances publiques mobilise depuis 2014 le ciblage de la fraude et la valorisation des requêtes (CFVR), avec un volume publiquement assumé représentant en 2024 près de la moitié des contrôles fiscaux des professionnels et 45 % des contrôles des particuliers (annexe III §5 ou §7 selon qualification). Les opérateurs sociaux exploitent des algorithmes de ciblage massifs, dont le code source a été publié en open data en janvier 2026 et qui font l'objet d'un contentieux porté par une coalition de vingt-cinq organisations devant le Conseil d'État (annexe III §5). Le

ministère de l'Intérieur poursuit l'expérimentation de la vidéosurveillance algorithmique prolongée par la loi jusqu'au 31 mars 2027 (article 5 et annexe III §6). La DINUM héberge sur Albert API près de cinquante produits administratifs, dont l'Assistant IA lancé en octobre 2025 auprès de dix mille agents dans huit ministères.

Aucun de ces déploiements ne dispose, au 22 mai 2026, d'une analyse d'impact sur les droits fondamentaux publique. Le constat ne disqualifie pas l'action des opérateurs concernés (l'obligation n'est pas encore applicable, l'instrument n'est pas encore outillé) mais il révèle un décalage temporel. À deux mois de l'entrée en application des obligations haut risque (le 2 août 2026, sauf report par le paquet Digital Omnibus européen présenté en novembre 2025), le SI public français ne dispose ni du template, ni de la doctrine nationale, ni de l'expérience consolidée pour produire des FRIA à grande échelle. La bascule par l'instrument se prépare en haut, le terrain n'est pas équipé en bas.

Conclusion : un paradoxe d'instrument à observer en 2027

Le paradoxe que ce dossier rend visible n'est pas un défaut de volonté, c'est un effet de structure. La CNIL prépare techniquement et juridiquement sa bascule. Le législateur a confié, dans le projet de DDADUE, les cas d'usage les plus sensibles à l'autorité que le Conseil d'État appelait dès 2022 à transformer en régulateur central de l'IA. L'autorité monte en puissance sanctionnatrice sur le secteur public, signal d'une exigence accrue. Le LINC mène, en partenariat avec le Centre for research in economics and statistics et le Centre de sociologie des organisations de Sciences Po, un programme de recherche sur l'explicabilité dont les premiers résultats, fondés sur l'analyse de plus de seize mille publications scientifiques, indiquent que la xAI ne parvient pas à un statut de production scientifique consensuelle. Ces signaux convergent vers un investissement réel.

L'angle mort se loge ailleurs. L'instrument « surveillance de marché » n'est pas l'instrument « droit fondamental ». Sa logique objective, descendante, industrielle, peut produire, par effet de structure, ce que Lascoumes et Le Galès appellent des « effets propres qui débordent les effets attendus ». L'enquête de conformité peut absorber la plainte de la personne concernée. L'évaluation de produit peut requalifier la garantie de droit. La coordination entre quinze autorités sectorielles, dans une tradition administrative française dont le palmarès en matière de coopération transversale n'est pas brillant, peut diluer une trajectoire que le législateur souhaitait recentrée.

L'hypothèse vérifiable est donc la suivante. À mai 2027, soit douze mois après l'application des obligations haut risque (sous réserve du Digital Omnibus), moins de 20 % des organismes publics français déployant des systèmes d'IA listés à l'annexe III auront publié une analyse d'impact sur les droits fondamentaux au sens de l'article 27 du règlement (UE) 2024/1689. L'indicateur observable est le recensement, à cette date, des FRIA disponibles sur les sites des opérateurs publics concernés et sur les portails des autorités de surveillance désignées.

Si l'hypothèse se confirme, elle signalera que la bascule par l'instrument s'est jouée en haut sans pénétrer le terrain, et que la régulation effective des systèmes d'IA publics français en 2027 ressemblera moins à un changement d'instrument qu'à une superposition d'instruments dont l'autorité dominante reste à déterminer.

Note méthodologique

Cette note s'appuie sur les sources institutionnelles primaires (CNIL, Sénat, Conseil d'État, DINUM, ministère de l'Économie, AESIA) confirmées par recherche directe, et sur la presse spécialisée (Banque des Territoires, Acteurs Publics) recoupée avec les comptes rendus officiels. Trois choix éditoriaux ont été tranchés. Le concept central retenu (instrumentation de l'action publique chez Lascoumes et Le Galès) a été préféré à d'autres lectures possibles (gouvernementalité chez Foucault, *tools of government* chez Hood, sociologie de la traduction chez Callon) pour sa capacité à articuler le changement d'instrument et son effet sur la définition même du problème régulé. Le parallèle historique principal mobilisé est interne à la CNIL (1978 / 2018 / 2026) plutôt que comparatif (AESIA, BNetzA), parce que la proximité structurelle avec l'objet analysé est maximale. Les déploiements d'IA dans la sphère des opérateurs sociaux ont été mentionnés en référence générique sans focus nominatif, en application du protocole de conflit d'intérêt déclaré. La mention par Next.ink, citant Contexte, du fondement *non bis in idem* invoqué par le Conseil d'État pour appuyer le revirement gouvernemental de février 2026 n'a pas été confirmée directement à partir d'un avis du Conseil d'État ou d'une pièce officielle du dossier législatif.

Sources

Sources primaires institutionnelles

CNIL, « Accompagnement des professionnels : le programme de travail de la CNIL pour 2026 », 7 avril 2026.

CNIL, « IA : la CNIL finalise ses recommandations sur le développement des systèmes d'IA et annonce ses futurs travaux », 22 juillet 2025. URL : https://www.cnil.fr/fr/ia-finalisation-recommandations-developpement-des-systemes-ia

CNIL, « Les contrôles en 2026 : recrutement, répertoire électoral unique et fédérations sportives », 3 avril 2026. URL : https://www.cnil.fr/fr/controles-prioritaires-2026

CNIL et Haute Autorité de santé, « Recommander les bonnes pratiques. Accompagner le bon usage des systèmes d'IA en contexte de soins », guide en consultation publique, mars 2026. URL : https://www.cnil.fr/sites/default/files/2026-03/guide_has_cnil_recommandations_ia.pdf

CNIL, « Informatique et Libertés : retour sur la création de la CNIL pendant le mandat du Président Valéry Giscard d'Estaing ». URL : https://www.cnil.fr/fr/loi-informatique-et-libertes-creation-mandat-valery-giscard-destaing

LINC (CNIL), « Why take an interest in the sociology of xAI science? [3/3] ». URL : https://linc.cnil.fr/en/why-take-interest-sociology-xai-science-33

LINC (CNIL), « A new project on explainable artificial intelligence ». URL : https://linc.cnil.fr/en/new-project-explainable-artificial-intelligence

Sénat, compte rendu intégral, séance du 17 février 2026 (projet de loi DDADUE, examen de l'amendement n° 442). URL : https://www.senat.fr/seances/s202602/s20260217/s20260217019.html

Conseil d'État, étude « Intelligence artificielle et action publique : construire la confiance, servir la performance », 30 août 2022 (synthèse disponible via Landot Avocats).

Cadre réglementaire européen

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act), articles 5, 27, 70 et annexe III.

Comité européen de la protection des données, avis 28/2024 sur certains aspects de la protection des données liés au traitement de données à caractère personnel dans le contexte des modèles d'IA, décembre 2024.

Cadre théorique

Pierre Lascoumes et Patrick Le Galès (dir.), *Gouverner par les instruments*, Paris, Presses de Sciences Po, 2004. Référence éditoriale : https://www.lgdj.fr/gouverner-par-les-instruments-9782724609493.html

Pierre Lascoumes et Patrick Le Galès, « Pas d'action publique autonome sans instruments propres », *Revue française de science politique*, 2011/1. URL : https://www.cairn.info/revue-francaise-de-science-politique-2011-1-page-51.htm

Compte rendu critique de *Gouverner par les instruments*, *Revue française de science politique*, 2021/HS1. URL : https://shs.cairn.info/revue-francaise-de-science-politique-2021-HS1-page-374

Presse spécialisée

Banque des Territoires, « Le Sénat valide une régulation de l'IA en mode puzzle », février 2026. URL : https://www.banquedesterritoires.fr/le-senat-valide-une-regulation-de-lia-en-mode-puzzle

Portail RGPD, « Le programme de travail de la CNIL pour 2026 : accompagnement des professionnels et nouvelles recommandations ». URL : https://veille.portail-rgpd.com/actu/programme-travail-cnil-2026-accompagnement-professionnels-recommandations/

Adequacy, « Privacy & AI Act : les 9 actus de février 2026 à retenir ». URL : https://www.adequacy.app/en/blog/conformite-ai-act-rgpd-fevrier-2026

Legiscope, « Bilan CNIL 2025 et priorités 2026 : 83 sanctions, 486 M€ ». URL : https://www.legiscope.com/blog/bilan-cnil-sanctions-2025-priorites-2026.html

Delsol Avocats, « La CNIL publie son programme de travail 2026 en matière d'accompagnement des professionnels ». URL : https://www.delsolavocats.com/La-CNIL-publie-son-programme-de-travail-2026-en-matiere-d-accompagnement-des-professionnels

IT for Business, « La CNIL finalise ses recommandations sur l'IA ». URL : https://www.itforbusiness.fr/la-cnil-finalise-ses-recommandations-sur-lia-93029

Acteurs Publics, « Derrière l'échec médiatique d'Albert, un projet d'IA plus global qui s'ancre dans l'État ». URL : https://acteurspublics.fr/articles/de-chatbot-experimental-a-socle-interministeriel-pour-lia-de-letat-le-parcours-dalbert-ia/

Ministère de l'Économie, « Détection des fraudes, analyse de données : comment l'IA a fait son entrée à Bercy ». URL : https://www.economie.gouv.fr/actualites/detection-des-fraudes-analyse-de-donnees-comment-lia-fait-son-entree-bercy

DINUM ALLiaNCE, « Assistant IA ». URL : https://alliance.numerique.gouv.fr/produit/produits-interministeriels/assistant-ia/

Comparaisons européennes

MIAI Grenoble (Multidisciplinary Institute in Artificial Intelligence), « EU AI Act Implementation: France Still Without Designated National Competent Authorities ». URL : https://ai-regulation.com/eu-ai-act-implementation-france-still-without-designated-national-competent-authorities/

MIAI Grenoble, « EU AI Act Implementation: German Cabinet approved the German AI Bill ». URL : https://ai-regulation.com/eu-ai-act-implementation-german-cabinet-approved-the-german-ai-draft-bill/

Protección Data, « Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) ». URL : https://protecciondata.es/agencia-espanola-supervision-inteligencia-artificial-aesia/

Dipartimento per la Trasformazione Digitale, « Approvata in via definitiva la legge italiana sull'Intelligenza Artificiale ». URL : https://innovazione.gov.it/notizie/articoli/approvata-in-via-definitiva-la-legge-italiana-sull-intelligenza-artificiale/

Technology's Legal Edge, « State of the Act: EU AI Act implementation in key Member States ». URL : https://www.technologyslegaledge.com/2025/11/state-of-the-act-eu-ai-act-implementation-in-key-member-states/