

La Lettre de XXI Institut – Numérique et intelligence artificielle

Septembre 2026 · XXI Institut

Publication du 17 octobre 2026

Intelligence artificielle dans l'action publique

Rapport des inspections : mesurer le gain d'un usage d'IA avant de décider sa généralisation

Le rapport conjoint des inspections générales des finances, de l'administration et des affaires sociales, daté d'avril 2026 et publié le 2 juillet, distingue les assistants généralistes, les fonctions supports et les usages métiers. Sa synthèse relève une adoption hétérogène et insiste sur les coûts complets, l'organisation et l'évaluation. L'exposition théorique d'un métier à l'IA n'équivaut pas à un gain de productivité effectivement obtenu.[1]

Cette distinction doit guider le choix d'une expérimentation. Une aide à la synthèse documentaire, une suggestion de réponse et une orientation de dossiers n'affectent pas le service de la même manière. Le projet devrait identifier la tâche, les personnes qui en bénéficient et le résultat attendu. Réduire le temps d'une opération peut être utile, mais le gain disparaît si la vérification exige davantage de travail en aval. Une évaluation portant seulement sur la vitesse de production laisserait alors de côté une partie du coût réel.

La comparaison devrait partir d'un état initial documenté : volume de dossiers, temps consacré, erreurs observées et délai de réponse. Pendant le test, il faut distinguer les résultats simples et les situations atypiques. Une moyenne peut masquer les cas dans lesquels l'outil se trompe ou oblige un agent à reprendre entièrement son travail. L'évaluation devrait aussi intégrer la qualité du résultat pour l'utilisateur. Un courrier produit plus rapidement mais devenu moins compréhensible ne traduit pas nécessairement une amélioration du service.

Le coût complet comporte l'achat ou l'hébergement, la préparation des données, la formation, les contrôles et les évolutions de l'outil. Une solution gratuite à l'essai peut devenir coûteuse lorsque les usages augmentent ou que les documents doivent être reclassés. Pour décider le passage à l'échelle, il serait utile de comparer plusieurs scénarios de charge et de mesurer les opérations qui restent humaines. Le financement devrait couvrir ces opérations au lieu de supposer qu'elles seront absorbées sans conséquence par les équipes existantes.

Le rapport invite ainsi à traiter l'IA comme une transformation du travail. Une expérimentation réussie devrait rendre explicites les conditions de sa réussite : données disponibles,

compétences, contrôle et périmètre des tâches. La généralisation pourrait ensuite être décidée sur cette base, avec un suivi des effets dans la durée. Le nombre d'agents équipés reste une information de déploiement ; il ne prouve pas, à lui seul, une amélioration de la qualité ou de l'efficacité de l'action publique.

Notre IA : un assistant généralisé doit laisser à l'agent les moyens d'exercer son jugement

Le 16 juin 2026, la Direction interministérielle du numérique présente la stratégie Notre IA et annonce le déploiement d'outils de synthèse, transcription, traduction et compte rendu. Le communiqué affirme que l'IA assiste les agents sans automatiser seule les décisions concernant les citoyens. Le gain allant jusqu'à 16 % cité pour la synthèse documentaire est un résultat annoncé de tests, pas une économie garantie dans toutes les administrations.[2]

Le maintien du jugement humain suppose plus qu'une signature en fin de processus. L'agent doit disposer des documents, du temps et des compétences nécessaires pour vérifier la proposition. Si le résultat est accepté par défaut pour tenir un objectif de cadence, le contrôle peut devenir formel. Un déploiement devrait préciser les tâches confiées à l'outil, les cas exigeant une vérification renforcée et les situations dans lesquelles l'agent doit pouvoir revenir à un traitement sans assistance. Cette possibilité doit être praticable dans l'organisation du service.

La transcription illustre le problème. Un compte rendu peut attribuer une phrase au mauvais interlocuteur, omettre une réserve ou confondre une proposition et une décision. Le contrôle doit donc porter sur les passages qui créent des engagements et sur les personnes qui les valident. Une règle interne pourrait distinguer notes de travail, relevé de décision et document destiné à être diffusé. La rapidité de la transcription ne supprime pas la responsabilité de choisir le statut du document et son circuit d'approbation.

La généralisation appelle aussi une politique des données d'entrée. Les agents doivent savoir quels documents peuvent être transmis, dans quel environnement et avec quelles conséquences de conservation. Un outil présenté comme souverain ne dispense pas de définir les habilitations ni les usages autorisés. La formation devrait partir des situations de travail : dossier individuel, réunion contenant des informations confidentielles ou document reçu d'un tiers. Des consignes compréhensibles réduisent davantage l'incertitude qu'une interdiction générale accompagnée d'exceptions difficiles à retrouver.

Pour apprécier le déploiement, le service pourrait suivre les corrections nécessaires, les difficultés rencontrées et les usages abandonnés. Un abandon motivé peut révéler une limite utile à connaître, plutôt qu'un défaut d'adhésion de l'agent. L'objectif annoncé d'une IA humaine devient concret lorsque le professionnel comprend l'aide reçue et peut en discuter le résultat. La disponibilité de l'outil est une première étape ; la capacité de contrôle dans le travail quotidien est celle qui détermine la qualité du service.

Transparence depuis le 2 août : distinguer le fournisseur, le service utilisant l'IA et le contenu publié

Le communiqué de la Commission du 31 juillet 2026 annonce l'application, le 2 août, des obligations de transparence pour certains usages de l'IA. L'article 50 du règlement distingue l'information sur l'interaction, le marquage technique des sorties et la divulgation de certains contenus par les utilisateurs professionnels, appelés déployeurs. Ces obligations n'imposent pas une mention uniforme sur chaque document réalisé avec une aide numérique.[3], [4]

Pour un assistant conversationnel public, le premier examen porte sur l'interaction : l'utilisateur doit être informé qu'il échange avec un système d'IA, sauf lorsque cela est évident dans les conditions prévues par le texte. L'information doit être claire et accessible dès le premier contact. Elle ne doit pas laisser croire que l'outil possède le pouvoir de prendre une décision que le service ne lui a pas confié. Un message sur la nature du système devrait être accompagné d'une indication intelligible de ce qu'il peut faire et de la manière de joindre le service compétent.

Le marquage lisible par machine relève d'une autre obligation, portant sur les fournisseurs de systèmes générant des contenus. Le texte prévoit notamment une exception pour certaines fonctions de mise en forme standard ou sans modification substantielle des données d'entrée et de leur sens. Pour l'acheteur public, la question contractuelle est donc de savoir quelles fonctionnalités relèvent du dispositif et comment les marques sont conservées lors des exports. Une simple étiquette visible ne démontre pas que les exigences techniques applicables au fournisseur sont satisfaites.

Pour les textes publiés afin d'informer sur une question d'intérêt public, l'article 50 prévoit une exception à la divulgation lorsque le contenu a fait l'objet d'un examen humain ou d'un contrôle éditorial et qu'une personne assume la responsabilité éditoriale. La vérification ne doit pas être confondue avec une validation nominale sans lecture. Les hypertrucages, contenus audio ou visuels manipulés, relèvent de dispositions propres, avec une adaptation pour certaines œuvres artistiques. Il faut donc qualifier le contenu et l'usage avant de choisir la mention.[4]

La conséquence pratique est d'établir une cartographie simple des usages : outil, fournisseur, service utilisateur, public et type de sortie. Elle permet d'identifier la responsabilité de chacun et les informations à fournir. Les clauses d'achat et les procédures de publication peuvent ensuite être adaptées à ces usages. La transparence est utile si elle explique au destinataire ce qu'il reçoit ; elle perd sa portée lorsqu'une mention générale recouvre indifféremment une interaction automatisée, une correction de forme et une décision publique.

Décisions algorithmiques et droits des usagers

Vidéoprotection à Nice : l'autorisation des caméras ne suffit pas à autoriser l'analyse algorithmique

Le 30 janvier 2026, le Conseil d'État rejette le recours de Nice contre l'avis de la CNIL sur un dispositif détectant automatiquement les véhicules devant les écoles et alertant la police municipale. Les dispositions autorisant la vidéoprotection n'autorisaient pas, dans leur silence, une analyse algorithmique systématique des images. L'absence alléguée de qualification d'IA à haut risque ne changeait pas cette absence de base nationale.[5]

Le raisonnement distingue trois opérations : recueillir les images, les analyser automatiquement et utiliser le résultat pour intervenir. Une autorisation donnée pour la première ne couvre pas nécessairement les suivantes. Pour une collectivité, le dossier doit décrire précisément le traitement envisagé, sa continuité, ses critères de détection et les suites données à l'alerte. Présenter le dispositif comme une simple amélioration de caméras existantes peut masquer une modification importante des possibilités de surveillance et de la manière dont les personnes sont repérées.

Le fait qu'un agent intervienne après l'alerte ne supprime pas la question de la légalité de l'analyse préalable. Le contrôle humain peut limiter certaines erreurs, mais il ne crée pas une habilitation juridique. De même, la classification dans le règlement sur l'IA et le droit national de la surveillance répondent à des questions différentes. Une analyse de conformité doit donc rechercher les textes qui autorisent l'usage concret, puis examiner les garanties techniques et organisationnelles. Commencer par le seul niveau de risque de l'IA laisse cette première étape inachevée.

Le besoin opérationnel doit également être discuté. Une détection peut produire de faux positifs, manquer certains événements ou multiplier les sollicitations des agents. Avant tout déploiement légalement autorisé, une évaluation devrait porter sur les situations qui déclenchent l'alerte et sur les décisions qu'elle entraîne. La performance de détection ne se confond pas avec la pertinence de l'intervention. Le service doit pouvoir expliquer pourquoi une alerte est retenue, corrigée ou classée, et conserver des informations adaptées pour contrôler le dispositif.

L'arrêt ne rend pas illicite toute analyse automatisée dans toutes les circonstances. Il précise l'insuffisance de la base invoquée pour ce traitement. Pour les décideurs, l'enseignement est de qualifier chaque nouvelle fonctionnalité avant l'achat ou l'activation. Un objectif de protection des écoles peut être légitime sans rendre disponible n'importe quel moyen. La conception doit articuler finalité, habilitation et garanties dès le départ, afin de ne pas découvrir après l'investissement que la fonctionnalité essentielle ne peut être utilisée.

Données publiques, partage et réutilisation

Feuille de route de data.gouv.fr : des métadonnées complètes rendent les données trouvables, pas nécessairement exactes

Le 18 février 2026, data.gouv.fr annonce notamment l'amélioration du score de qualité des métadonnées, de la recherche et des parcours d'accès aux données restreintes. La publication présente une feuille de route susceptible d'évoluer, pas un bilan de toutes les fonctionnalités livrées. Le score concerne la description des jeux ; il ne démontre pas l'exactitude de chacune de leurs valeurs.[6]

Cette distinction est centrale pour la réutilisation administrative. Un fichier peut être bien décrit et contenir des erreurs ; un fichier exact peut rester inutilisable faute de définition des colonnes, de période ou d'échelle géographique. Le producteur doit donc traiter séparément la qualité des données et celle de leur présentation. Pour une politique publique, le réutilisateur devrait pouvoir comprendre la population couverte, les unités, les exclusions et les changements de méthode. Sans ces éléments, deux tableaux apparemment comparables peuvent conduire à une conclusion trompeuse.

La mise à jour demande également une information explicite. Une donnée actualisée peut intégrer une révision historique ou seulement une période supplémentaire. Les versions devraient permettre de savoir ce qui a changé et pourquoi. Une publication écrasant silencieusement le fichier précédent rend difficile la reproduction d'une analyse. Pour un service utilisant les données dans un indicateur, conserver le millésime et la méthode est une précaution de gestion : elle permet de distinguer l'évolution du phénomène d'une correction de la source.

L'intégration de données à accès restreint pose une autre question. Les rendre découvrables ne signifie pas les rendre librement téléchargeables. Le catalogue devrait expliquer les conditions d'accès, l'autorité compétente et les usages permis. La procédure d'habilitation doit être compréhensible pour le demandeur, tout en conservant les protections nécessaires. Une visibilité accrue peut faciliter la recherche, mais elle peut aussi créer des demandes inadaptées si les limites sont dissimulées derrière une présentation semblable à celle des données ouvertes.

Pour apprécier la feuille de route, un suivi utile porterait sur le temps nécessaire pour trouver une donnée, comprendre son champ et accomplir le parcours d'accès approprié. Le nombre de fichiers publiés reste insuffisant pour mesurer la réutilisation. L'objectif est de permettre une analyse fiable et reproductible. Le score de métadonnées peut contribuer à ce résultat, à condition d'être lu comme un outil d'amélioration de la documentation et non comme un label garantissant toute conclusion construite à partir du jeu.

Archive de presse et droit à l'oubli : l'ancienneté ne suffit pas à imposer suppression ou anonymisation

Le 3 juin 2026, la première chambre civile rejette le pourvoi n° 25-14.228 portant sur une archive de 20 Minutes. La demande de suppression puis d'anonymisation devait être appréciée en mettant en balance vie privée, données personnelles et liberté d'information. L'intérêt actuel de l'information, la notoriété, l'accessibilité et le préjudice allégué comptaient parmi les critères. Le rejet demeure lié à cette appréciation concrète.[7]

La conservation et la facilité de recherche sont deux dimensions différentes. Un contenu peut rester dans une archive tout en devenant moins accessible depuis un moteur ; une recherche interne peut, inversement, continuer à exposer fortement une personne. Pour apprécier une demande, le dossier doit décrire ces conditions d'accès plutôt que se limiter à la date de l'article. L'objet exact de la mesure compte aussi : suppression du contenu, retrait d'un nom et modification du référencement ne produisent pas les mêmes effets sur l'information du public.

La personne demandant une modification doit préciser les conséquences qu'elle invoque. Une difficulté professionnelle, une confusion persistante ou une reprise massive peuvent appeler des éléments de preuve différents. Pour l'éditeur, l'intérêt contemporain doit être expliqué à partir du sujet et du rôle du nom dans l'information. La seule origine journalistique ne suffit pas à résoudre automatiquement chaque demande. Une réponse motivée devrait rendre visibles les éléments de la mise en balance et distinguer ceux qui sont établis de ceux qui restent allégués.

L'arrêt rappelle aussi que la dispense d'inscription d'une condamnation au bulletin n° 2 du casier judiciaire n'équivaut pas à une interdiction générale de connaître cette condamnation. Les fonctions du casier et celles de l'archive ne se confondent pas. Cela n'élimine pas la protection de la vie privée ; cela empêche de déduire de la première mesure une obligation automatique de suppression. Une analyse rigoureuse doit rattacher la conséquence demandée au mécanisme juridique pertinent, sans faire circuler une décision d'un domaine à l'autre comme si elle avait le même objet.

Pour les organismes diffusant de l'information, le résultat plaide pour un circuit individualisé de traitement des demandes. Il devrait permettre de vérifier la version du contenu, l'état du référencement et les raisons de conserver l'identification. Le droit à l'oubli ne signifie ni disparition automatique de toute archive ancienne ni conservation intangible. La qualité du traitement tient à une comparaison précise des droits et des effets de la mesure, dans les circonstances actuelles de la diffusion.

Analyse pseudonymisée : la recevabilité de la preuve dépend de ses modalités, pas de son seul intitulé

Le 17 juin 2026, la chambre commerciale rejette le pourvoi n° 25-11.499 dans un litige électoral chez Orange. L'analyse technique avait pseudonymisé les données, détruit les données initiales et étudié des volumes sans contenu de courriels ni fichier nominatif. La production était jugée nécessaire et proportionnée. La pseudonymisation seule ne suffit donc pas à rendre admissible toute collecte ou toute preuve.[8]

Le raisonnement intéresse les investigations numériques parce qu'il examine l'atteinte réellement produite. Une analyse du nombre d'échanges et une lecture du contenu ne révèlent pas les mêmes informations. Un fichier pseudonymisé peut néanmoins permettre des rapprochements sensibles si les clés ou d'autres sources restent disponibles. Le dossier doit expliquer les opérations et leurs limites. Une attestation se bornant à employer le mot pseudonymisation ne permet pas d'apprécier ce que les enquêteurs ont effectivement vu ou conservé.

Le besoin de preuve doit être défini avant la recherche. Pour comprendre une fuite, il peut être nécessaire d'examiner des traces techniques déterminées ; cela ne justifie pas automatiquement l'extraction de toutes les communications. Un protocole pourrait préciser le périmètre, la période, les données exclues et le résultat attendu. Cette préparation facilite ensuite la discussion de la proportionnalité. Elle permet aussi de conserver une preuve exploitable sans accumuler des informations sur des tiers qui n'apportent rien à la question posée.

La traçabilité du travail est une garantie importante. Les personnes qui discutent le rapport doivent pouvoir comprendre la méthode, les traitements réalisés et les limites de l'interprétation. La destruction de certains originaux peut limiter l'atteinte, mais elle demande d'organiser la possibilité de vérifier les résultats selon les modalités pertinentes. Le protocole doit donc concilier minimisation et contrôle de la preuve. Une opération techniquement sophistiquée reste contestable si ses étapes et ses conclusions ne peuvent être expliquées.

L'arrêt n'accorde pas un droit général de produire des données au motif qu'un litige existe. Il confirme une appréciation des besoins et des garanties dans cette affaire. Pour une administration ou un organisme, l'enseignement est de préparer les investigations comme un traitement délimité, avec des responsabilités et une méthode vérifiable. La sécurité juridique vient de cette articulation entre nécessité et limites ; elle ne résulte pas du seul changement d'identifiant dans un fichier.

Souveraineté numérique et infrastructures

Doctrine cloud de l'État : une réversibilité contractuelle doit être financée pour devenir utilisable

Le choix de l'hébergeur de la Plateforme des données de santé annoncé le 21 mai 2026 remet au premier plan les règles de la doctrine cloud de l'État. Sa règle 4 demande des conditions de sortie soutenables et des ressources financières, techniques et humaines provisionnées dès le lancement ; les règles 5 et 10 traitent de résilience et de portabilité. Une clause de sortie ne démontre pas que la migration sera praticable.[9], [10]

La réversibilité comporte plusieurs opérations : exporter les données, récupérer leur documentation, remplacer les services spécifiques et vérifier le fonctionnement chez le nouvel hébergeur. L'export d'un fichier peut être facile alors que la reprise des droits d'accès, des automatisations ou des interfaces est coûteuse. Un marché devrait donc décrire les éléments à

restituer et les prestations de transition, avec leurs formats et leurs délais. La liberté de changer de fournisseur dépend de cet ensemble, pas seulement de la propriété nominale des données.

Le coût doit être évalué avant que la dépendance soit installée. Une fonctionnalité propre à un fournisseur peut rendre un service plus performant aujourd'hui tout en augmentant la charge de sortie. Ce compromis peut être assumé, mais il doit être explicite. Une comparaison des offres devrait intégrer le coût total sur la durée, les scénarios de croissance et la migration possible. Une économie immédiate perd une partie de son sens si elle rend toute évolution ultérieure financièrement hors de portée.

La continuité demande un test distinct. Le service doit savoir combien de temps la migration peut interrompre les fonctions essentielles et quelles opérations peuvent se poursuivre pendant ce délai. Des sauvegardes disponibles ne garantissent pas la reprise si les équipes ne savent pas les restaurer ou si les logiciels nécessaires manquent. Un exercice limité à un jeu de données et à quelques fonctionnalités peut révéler des dépendances ignorées. Il aide à transformer la documentation contractuelle en capacité opérationnelle.

La doctrine concerne l'organisation du numérique de l'État ; elle ne doit pas être présentée comme une obligation identique de chaque acteur privé. Elle offre toutefois une manière précise d'apprécier un achat public critique. Les moyens de sortie doivent être connus, financés et entretenus. À mesure que le produit évolue, la documentation et les tests doivent suivre. Une réversibilité prévue une seule fois au lancement peut devenir fictive si les fonctionnalités et les données se développent sans réexamen.

Données de santé : distinguer le choix du futur hébergeur et la légalité d'un traitement déjà autorisé

La DINUM décrit le 8 juin 2026 le choix de Scaleway annoncé par la Plateforme des données de santé le 21 mai, avec une migration et des tests encore à conduire. Le 20 mars, dans les affaires nos 503159 et 504171 relatives à DARWIN EU, le Conseil d'État avait rejeté les recours contre un traitement autorisé sur l'infrastructure existante, en distinguant données de santé hébergées en France et données techniques d'usage.[9], [11]

Ces deux faits répondent à des questions différentes. Le choix d'une infrastructure future peut poursuivre un objectif de maîtrise technologique ; le contrôle d'une autorisation examine un traitement défini et ses garanties à la date pertinente. Une décision favorable sur ce traitement ne certifie pas tous les usages de l'infrastructure. À l'inverse, la volonté de changer d'hébergeur ne démontre pas que chaque autorisation antérieure était illégale. La portée de chaque décision reste donc limitée au traitement examiné et aux garanties retenues.

L'examen des flux est déterminant. Les données d'étude, les comptes des utilisateurs, les journaux techniques et les informations de support ne suivent pas nécessairement les mêmes circuits. Le dossier devrait préciser leur contenu, leur destination et les accès possibles. Une affirmation globale selon laquelle les données sont en France peut laisser de côté des flux techniques ; une affirmation globale de transfert peut, inversement, attribuer aux données de

santé un mouvement qui concerne seulement des informations d'usage. La cartographie doit permettre de vérifier ces distinctions.

Pour la migration, les garanties doivent être reprises et testées sur la nouvelle organisation. Il faut identifier les responsabilités, les accès, les durées de conservation et les risques de réidentification. Le Conseil d'État avait apprécié un ensemble de mesures et une autorisation limitée à trois ans ; ces éléments ne sont pas transférables automatiquement à n'importe quel nouveau traitement. Le changement d'hébergeur est donc un projet de sécurité et de continuité, avec des validations correspondant aux opérations réellement réalisées.

L'information publique devrait rendre visibles les étapes : sélection, préparation, transfert, validation et mise en service. L'annonce du choix ne signifie pas que toutes les données ont déjà migré. Un suivi concret pourrait préciser les tests achevés, les dépendances restant à traiter et les garanties vérifiées. Cette présentation permet de discuter la souveraineté à partir des capacités obtenues, sans confondre orientation stratégique, conformité d'un dossier particulier et résultat opérationnel d'une transition encore en cours.

Rapport Arcep 2026 : la liberté de changer de cloud dépend aussi des coûts et des formats

Le 16 juillet 2026, l'Arcep présente son rapport sur l'état de l'internet et revient sur la recommandation relative à la portabilité et à l'interopérabilité cloud. Le communiqué mentionne aussi une proposition adressée au Gouvernement concernant les frais de transfert. Cette proposition ne doit pas être assimilée, sur le seul fondement du communiqué, à une nouvelle règle tarifaire déjà adoptée.[12]

La liberté de changer de fournisseur doit être appréciée à partir d'un scénario complet. L'utilisateur doit récupérer les données, les adapter à l'environnement d'arrivée et remettre le service en fonctionnement. Un transfert peu coûteux peut rester difficile si les formats ou les interfaces diffèrent. À l'inverse, une compatibilité technique peut perdre son intérêt lorsque le coût de migration est prohibitif. Une évaluation utile rapprocherait les deux dimensions au lieu d'en faire des critères indépendants dans une comparaison d'offres.

Pour les acheteurs publics, le contrat devrait expliciter les frais, les délais et les services d'assistance à la sortie. Les changements de volume et l'évolution des fonctionnalités doivent être anticipés. Une tarification lisible au lancement peut devenir incertaine si l'export dépend de prestations complémentaires mal définies. L'acheteur a intérêt à demander un exemple de migration et à vérifier les limites de l'offre. Un engagement abstrait d'interopérabilité ne renseigne pas suffisamment sur le travail nécessaire pour reprendre le produit.

Le suivi du marché devrait également conserver la documentation des dépendances. Les équipes peuvent adopter progressivement des services spécifiques parce qu'ils facilitent le développement. Cette évolution doit être enregistrée et discutée au regard du coût de sortie. La portabilité n'est pas un état définitif acquis lors de la signature ; elle peut se réduire au fil des choix techniques. Une revue périodique permet d'identifier les adhérences nouvelles et de décider si leur bénéfice justifie les moyens nécessaires à une migration ultérieure.

Le communiqué de l'Arcep donne une perspective de régulation, mais ne remplace pas l'analyse du contrat particulier. Pour apprécier l'ouverture du marché, il faudrait aussi observer les migrations effectivement réalisées et les obstacles rencontrés. La diversité des fournisseurs disponibles ne garantit pas qu'un client puisse les rejoindre. La liberté de choix devient réelle lorsque les conditions économiques et techniques de la transition sont suffisamment précises pour être testées et utilisées.

Plateformes et régulation numérique

AliExpress : la sanction vise l'évaluation et la réduction des risques, au-delà du retrait d'une annonce

Le 20 juillet 2026, la Commission annonce une amende de 550 millions d'euros contre AliExpress au titre du règlement sur les services numériques, dit DSA. Le communiqué vise des insuffisances d'évaluation et de réduction des risques liés aux produits illégaux, dangereux ou contrefaits, et demande des actions correctrices. Le montant de l'amende ne démontre pas que ces corrections seraient déjà exécutées.[13]

Le raisonnement de régulation dépasse la seule annonce problématique. Une plateforme doit être appréciée aussi selon l'organisation qui permet la diffusion répétée de produits présentant un risque. Pour analyser cette organisation, il faut regarder les contrôles d'entrée, les signalements, les réactions aux récidives et les incitations commerciales. Supprimer une annonce peut être nécessaire sans résoudre le mécanisme qui lui permet de réapparaître. Une mesure corrective devrait donc être reliée au risque qu'elle cherche à réduire et aux résultats attendus.

L'évaluation appelle des données adaptées. Compter les retraits ne suffit pas si le volume de produits dangereux augmente, si les mêmes vendeurs reviennent ou si les signalements sont traités trop tard. Un suivi devrait permettre de distinguer prévention, détection et correction. Les indicateurs peuvent porter sur le délai, les contrôles effectués et la récurrence des cas. Ils doivent aussi préciser le périmètre : une proportion calculée sur les seuls signalements ne décrit pas nécessairement tous les produits accessibles sur le service.

Pour les autorités et les utilisateurs, la transparence sur les corrections est donc importante. Une annonce de renforcement des contrôles doit être rapprochée de leur déploiement et de leur efficacité. Les engagements devraient décrire les pratiques modifiées et permettre une vérification. Cela ne signifie pas qu'une plateforme pourrait garantir l'absence absolue de tout produit illicite ; cela signifie que l'examen doit porter sur les obligations et les mesures effectivement mises en œuvre pour les risques identifiés.

Le cas rappelle enfin que sanction et suivi ont des fonctions distinctes. L'amende répond aux manquements constatés, tandis que la décision corrective cherche à modifier la situation. Pour un lecteur, l'objet de l'actualité ne se réduit donc pas au chiffre annoncé. La question suivante est celle des changements obtenus dans le fonctionnement du service et des moyens permettant d'en contrôler la permanence, sans présumer que la procédure de suivi est achevée.

Facebook et Instagram : les constats préliminaires portent aussi sur la conception du service

Le 10 juillet 2026, la Commission annonce des constatations préliminaires concernant la conception addictive de Facebook et Instagram. Elle vise notamment le défilement continu, la lecture automatique, les notifications et les recommandations personnalisées, ainsi que les risques pour les mineurs et les adultes vulnérables. Le statut préliminaire doit être conservé : le communiqué n'annonce pas une sanction définitive de ces fonctionnalités.[14]

Cette approche déplace l'analyse du contenu vers les conditions dans lesquelles il est proposé. Une interface peut encourager la poursuite de l'usage sans produire elle-même un contenu illégal. Le débat porte alors sur l'évaluation des risques et les mesures destinées à les réduire. Pour comprendre le service, il faut examiner le parcours de l'utilisateur : comment il entre, comment le suivant est présenté et quelles possibilités réelles lui sont offertes pour interrompre ou modifier l'expérience. Le nom d'une fonctionnalité ne suffit pas à établir son effet.

La discussion devrait également distinguer les publics. Un paramètre pouvant être compris et modifié par un adulte averti peut être moins accessible à un mineur ou à une personne vulnérable. Les mesures proposées doivent être appréciées dans ces conditions d'usage. Un bouton de désactivation peu visible n'a pas la même portée qu'un choix présenté clairement lors de la configuration. Le contrôle doit donc s'intéresser à la disponibilité de l'option, à sa compréhension et à son utilisation, plutôt qu'à sa seule existence dans les paramètres.

Le caractère préliminaire laisse place à une réponse de l'opérateur et à la poursuite de l'examen. Une information juridique rigoureuse doit attribuer les constats à la Commission et éviter de les convertir en faits définitivement jugés. Pour les concepteurs d'autres services, cette distinction n'empêche pas de tirer une question de travail : les mécanismes de sollicitation sont-ils évalués selon leurs effets sur les utilisateurs ? L'analyse peut être engagée sans affirmer que la même qualification s'appliquerait automatiquement à toute interface similaire.

L'intérêt de cette actualité est d'introduire la conception dans le champ du suivi des risques numériques. Les corrections peuvent porter sur des choix de navigation et de recommandation, pas seulement sur une politique de modération. Leur efficacité devrait ensuite être examinée avec des données sur les usages. Le contrôle conserve ainsi deux exigences : comprendre les effets du service et respecter les étapes de la procédure avant d'annoncer une responsabilité définitivement établie.

Tagadamedia : un bouton de validation ne garantit pas un consentement libre et compréhensible

Le 20 mai 2026, le Conseil d'État ramène à 50 000 euros l'amende infligée à Tagadamedia. Un grief avait été substitué à celui du rapport sans permettre une réponse. Les autres manquements sur les formulaires de consentement et l'injonction sont maintenus : mise en valeur du bouton de validation et ambiguïtés du refus empêchaient un consentement valable. La réduction ne valide donc pas les interfaces contestées.[15]

La décision distingue la garantie procédurale du contrôle de fond. Une autorité doit permettre à l'organisme de répondre au grief qu'elle retient ; les mêmes faits ne rendent pas interchangeables toutes les qualifications juridiques. L'annulation sur un point ne signifie pas que les autres manquements disparaissent. Pour analyser une sanction, il faut identifier ce qui a été annulé, ce qui est maintenu et la conséquence sur le montant. Une présentation globale de victoire ou de validation perdrait ces éléments utiles.

Sur l'interface, l'acte positif n'est qu'une partie du consentement. L'utilisateur doit comprendre l'usage des données et disposer d'un choix suffisamment clair. Le contrôle porte donc sur la taille, la mise en valeur, les formulations et le parcours réel. Une information accessible par un lien peut aider sans corriger une ambiguïté présente au moment de cliquer. Pour un organisme, tester le formulaire avec des utilisateurs permet d'identifier les conséquences qu'ils pensent accepter et celles qu'ils ne voient pas.

La conservation des versions est également importante. Les conditions d'une collecte peuvent évoluer entre deux contrôles ou deux campagnes. Pour démontrer le choix d'une personne, il faut pouvoir rapprocher son action du formulaire et de l'information correspondants. Un modèle actuel correctement rédigé ne prouve pas la qualité des collectes anciennes. Le service devrait conserver une documentation proportionnée sur les versions, les parcours et les usages annoncés, afin de répondre à une demande sans reconstruire après coup l'expérience présentée à l'utilisateur.

Pour les plateformes et services numériques, l'arrêt invite à traiter le consentement comme une situation de compréhension et de choix. Un bouton coché ne résout pas automatiquement la question. La procédure de contrôle et la qualité du parcours doivent toutes deux être respectées. L'intérêt pratique est d'examiner les écrans effectivement utilisés, puis les preuves conservées, au lieu de considérer une formule juridique insérée dans une politique générale comme suffisante pour toute collecte.

Cybersécurité et continuité des services

REACTIV : préparer les décisions locales pour rendre l'intervention interministérielle efficace

Le 7 septembre 2026, l'Agence nationale de la sécurité des systèmes d'information annonce REACTIV, une capacité renforcée de réaction aux compromissions de comptes et aux violations de données dans les services de l'État. L'appui aux ministères et une communication technique de crise centralisée sont annoncés. Le dispositif concerne ce périmètre ; il ne constitue pas une garantie d'intervention identique pour tout organisme public ou privé.[16]

Une capacité centrale ne produit ses effets que si l'organisme peut agir rapidement. Lors d'une compromission de compte, il faut identifier les accès, décider leur suspension, conserver les éléments utiles et vérifier les systèmes touchés. Une équipe extérieure peut apporter une expertise, mais elle ne connaît pas nécessairement toutes les dépendances métier. Le service doit donc préparer les personnes habilitées à décider et les informations à transmettre. Une liste

de contacts obsolète ou un pouvoir de décision incertain peut retarder les mesures les plus urgentes.

La réponse doit aussi articuler sécurité et continuité. Fermer un accès ou isoler un système peut limiter l'attaque tout en interrompant une mission essentielle. Les responsables doivent savoir quelles fonctions peuvent continuer par un autre moyen et quelles décisions nécessitent un arbitrage. Un plan de crise utile décrit ces situations, les ressources nécessaires et le circuit d'information. Il ne devrait pas se réduire à une procédure technique de coupure dépourvue d'analyse des conséquences sur les agents et les usagers.

La communication technique centralisée ne remplace pas toutes les obligations d'information ou de notification. Les organismes doivent qualifier l'incident et examiner les règles qui leur sont applicables, notamment lorsque des données personnelles sont concernées. Le suivi devrait séparer ce qui est connu, ce qui est suspecté et ce qui reste à vérifier. Une information prématurément rassurante peut être démentie par l'analyse ; une communication indifférenciée peut, inversement, attribuer à toutes les données un risque qui n'a pas été établi.

Pour préparer l'usage du dispositif, un exercice pourrait partir d'un compte compromis puis suivre la détection, l'alerte, les décisions et la reprise. L'objectif serait de vérifier la chaîne réelle plutôt que la présence d'un document de crise. REACTIV apporte une capacité annoncée d'assistance ; les administrations doivent conserver les moyens de l'utiliser. La rapidité repose sur cette préparation partagée, où responsabilités techniques, décisions de service et communication sont identifiées avant l'incident.

Cybermenace 2025 : la baisse des événements traités par l'ANSSI ne mesure pas toute la menace

Le panorama présenté le 11 mars 2026 indique que l'ANSSI a traité 3 586 événements de sécurité en 2025, soit 18 % de moins qu'en 2024. La présentation évoque notamment les pics de signalements liés aux Jeux de Paris. Elle souligne en parallèle les exfiltrations et les compromissions d'équipements exposés. Ce décompte d'activité ne recense pas toutes les attaques subies en France.[17]

La lecture des chiffres exige de comprendre leur production. Un événement porté à la connaissance d'une agence dépend des capacités de détection, du comportement de signalement et du périmètre d'intervention. Une baisse peut donc avoir plusieurs significations. Elle ne démontre pas automatiquement une diminution du risque pour un organisme particulier. Pour comparer les années, il faut examiner les circonstances exceptionnelles et les catégories suivies. L'indicateur reste utile, à condition de ne pas lui attribuer une couverture qu'il n'a pas.

Le service doit ensuite rapprocher la menace de ses propres dépendances. Un organisme exposé à une fuite de données, une indisponibilité ou une altération des décisions ne prépare pas exactement les mêmes réponses. Une analyse de risques devrait identifier les fonctions essentielles, les accès externes et les conséquences d'un incident. Une statistique nationale ne remplace pas cet inventaire. Elle peut aider à choisir les scénarios à tester et à repérer les équipements ou les comptes qui méritent un contrôle prioritaire.

Les exfiltrations demandent une attention distincte de la seule continuité. Un service peut reprendre son fonctionnement alors que les données copiées restent exposées. La restauration ne fait pas disparaître cette conséquence. Le suivi devrait donc distinguer rétablissement technique, qualification de la fuite et accompagnement des personnes concernées. Les preuves conservées doivent permettre d'expliquer ce qui a été consulté ou extrait, sans transformer une suspicion initiale en certitude ni conclure à l'absence de fuite faute de trace disponible.

L'intérêt du panorama est de fournir des scénarios et des points d'attention, plutôt qu'un chiffre rassurant ou alarmant pris isolément. Une politique de sécurité peut ensuite définir des priorités vérifiables : protection des comptes, correction des vulnérabilités, visibilité des traces et exercices de reprise. Le résultat doit être apprécié sur les risques propres au service. La diminution du nombre d'événements traités par une agence ne dispense pas de vérifier ces capacités dans l'organisme qui décide de ses moyens.

Cyber Resilience Act : le signalement des fabricants commence avant la pleine application des obligations produit

Depuis le 11 septembre 2026, l'article 14 du règlement sur la cyberrésilience, ou Cyber Resilience Act, prévoit des notifications par les fabricants concernant les vulnérabilités activement exploitées et les incidents graves affectant la sécurité des produits. L'article 71 distingue cette échéance de l'application générale au 11 décembre 2027. La plateforme unique transmet les signalements aux acteurs compétents ; l'ANSSI en présente le fonctionnement français.[18], [19]

Cette chronologie évite une erreur de périmètre. Le début d'une obligation de notification ne signifie pas que toutes les obligations de conception, de documentation et de conformité sont déjà applicables. Il faut identifier la qualité de l'acteur, le produit concerné et l'obligation considérée. Un acheteur public utilisant un logiciel ne devient pas fabricant pour ce seul motif. Il peut cependant devoir obtenir de son fournisseur des informations permettant de comprendre un incident et d'examiner ses propres obligations.

Le signalement des vulnérabilités activement exploitées et celui des incidents graves suivent des séquences prévues par l'article 14, comprenant une alerte précoce puis des informations complémentaires. Le fabricant doit donc organiser la remontée des faits et la capacité de qualifier l'événement. Un circuit reposant sur une seule personne indisponible peut rendre le délai difficile à tenir. Les équipes chargées du produit, de la sécurité et des obligations juridiques doivent partager les critères et le point de départ du traitement.[19]

Pour l'utilisateur d'un produit critique, le contrat pourrait préciser les informations attendues : versions affectées, mesures temporaires, correctifs et conditions de déploiement. Recevoir un avis ne suffit pas si l'organisme ne sait pas où le produit est utilisé ou ne peut pas appliquer la mesure. L'inventaire des composants et des dépendances devient alors un outil de continuité. La préparation devrait permettre de rapprocher une alerte fournisseur des services réellement exposés et des personnes pouvant décider l'action nécessaire.

Le règlement crée un cadre de responsabilité produit ; il ne se confond pas avec tous les régimes de notification d'incidents ou de violations de données. Un même événement peut soulever plusieurs obligations, qui doivent être examinées chacune selon leur champ. L'intérêt immédiat de l'échéance de septembre est de rendre cette coordination opérationnelle. Le suivi doit préciser qui signale, qui reçoit, qui décide la correction et comment le service vérifie que le produit exposé a effectivement été traité.

Appel du G7 sur le post-quantique : commencer par l'inventaire des usages cryptographiques

Le 3 septembre 2026, l'ANSSI présente l'appel à l'action de ses partenaires du G7 sur la transition vers la cryptographie post-quantique. L'objectif est de préparer les organisations à des algorithmes résistants aux attaques quantiques. Il s'agit d'une orientation de préparation ; la publication ne fixe pas, à elle seule, une obligation juridique universelle de remplacer immédiatement tous les systèmes.[20]

La première difficulté est de savoir où la cryptographie est utilisée. Elle protège des connexions, des signatures, des sauvegardes et des échanges entre applications, parfois dans des composants peu visibles. Un inventaire devrait identifier les usages, les fournisseurs et les possibilités de mise à jour. Sans cette connaissance, une migration peut être décidée sur les outils les plus apparents tout en laissant intacts des dépendances essentielles. Le besoin de préparation ne se réduit donc pas à choisir un nouvel algorithme.

La durée de sensibilité des informations doit orienter la priorité. Des données conservant longtemps leur valeur peuvent poser une difficulté différente de documents rapidement périmés. La planification devrait rapprocher cette durée du cycle de renouvellement des équipements et des logiciels. Un système qui ne peut évoluer qu'à l'occasion d'un remplacement matériel demande une anticipation particulière. L'analyse ne suppose pas de prédire une date certaine d'attaque ; elle permet de décider quelles dépendances seraient les plus coûteuses à traiter tardivement.

La transition devra également être testée dans les chaînes d'échange. Un service peut adopter un mécanisme nouveau tout en devant communiquer avec des partenaires qui ne le supportent pas encore. Les effets sur la performance, les certificats et les opérations d'administration doivent être évalués. Une expérimentation limitée peut révéler les incompatibilités avant le basculement. Le contrat devrait aussi prévoir l'information sur la feuille de route du fournisseur et les conditions d'évolution, afin de ne pas découvrir l'impossibilité de migrer à la fin du marché.

L'intérêt de l'appel est d'engager ce travail de préparation maintenant, sans présenter une recommandation comme un ordre réglementaire déjà applicable à tous. Une trajectoire pourrait définir les usages prioritaires, les tests, les dépendances et les décisions d'achat à venir. Elle devrait être révisée selon les progrès des solutions et les informations disponibles. La maîtrise du risque passe par une capacité d'évolution documentée ; une annonce de migration dépourvue d'inventaire ne démontre pas que les points critiques ont été identifiés.

Accès et inclusion dans les services numériques

ANEF : l'accompagnement ne suffit pas lorsque le logiciel empêche la démarche elle-même

Le 5 mai 2026, le Conseil d'État ordonne de corriger plusieurs blocages de l'Administration numérique pour les étrangers en France, dite ANEF. Il distingue l'aide au maniement du portail et la solution de substitution en cas d'impossibilité technique. L'annulation porte sur des refus précisément identifiés, avec des délais depuis la notification ; elle ne constate pas que tous les griefs seraient établis à l'échelle nationale.[21]

L'inclusion numérique comporte donc deux situations différentes. Une personne peut avoir besoin d'aide pour remplir un formulaire disponible ; elle peut aussi savoir l'utiliser et être bloquée par sa conception. Une permanence d'accompagnement répond à la première difficulté, mais pas nécessairement à la seconde. L'évaluation devrait rechercher ce qui empêche la démarche : équipement, compréhension, identité du compte, changement de situation ou fonction absente. Une réponse uniforme risque de renvoyer plusieurs fois la personne vers un parcours qui ne permet pas de résoudre le problème.

La solution de substitution doit préserver la possibilité de déposer la demande et d'en obtenir une preuve. Elle ne devrait pas devenir une succession de rendez-vous sans responsable identifiable. Pour le service, le circuit doit préciser comment l'échec est constaté, comment le dossier est transmis et comment l'utilisateur sait qu'il a été enregistré. La continuité du droit dépend de ces opérations concrètes. Un accueil organisé peut rester insuffisant si la personne reçue ne peut pas accomplir la formalité dans le délai pertinent.

La conception doit également permettre les événements intervenant pendant l'instruction. Un changement d'adresse ou une nouvelle pièce peuvent affecter la décision ; le portail doit disposer d'un circuit adapté. La qualité du formulaire initial ne garantit pas celle du parcours sur plusieurs mois. Un test utile devrait suivre un dossier depuis son dépôt jusqu'à la réponse, en incluant ces événements. Les corrections doivent être vérifiées avec des situations réelles de traitement, pas seulement avec une démonstration technique sans conséquences sur les droits.

Pour les autres téléservices, la décision ne peut être transposée mécaniquement dans tous ses détails. Elle fournit néanmoins une question d'évaluation précise : le service permet-il les démarches que les textes reconnaissent, y compris lorsque l'outil échoue ? Un suivi de l'inclusion devrait donc mesurer les démarches effectivement accomplies et les blocages résolus. Le nombre de personnes accompagnées est utile, mais il ne prouve pas que leur accès au droit a été rétabli.

Communication pénale : une adresse joignable n'est pas nécessairement un canal de dépôt recevable

Le 27 mai 2026, la chambre criminelle rejette le pourvoi n° 26-81.526. Une demande de pièces pouvait être faite par lettre, mais son envoi électronique devait respecter le canal prévu ; l'adresse utilisée n'était pas éligible à la communication pénale. La Cour relève aussi que la demande n'avait pas été réitérée dès l'ouverture du débat. L'arrêt ne constate pas un accès inconditionnel par tout courriel au greffe.[22]

La distinction est importante pour la conception des services numériques. Une boîte de contact peut servir à échanger une information sans permettre le dépôt d'un acte de procédure. Si cette différence n'est pas visible, un utilisateur peut recevoir une apparence de transmission réussie tout en perdant l'effet juridique attendu. Le service devrait donc indiquer les usages de chaque canal et orienter vers celui qui convient. Une réponse automatique accusant réception ne devrait pas laisser croire qu'elle certifie la recevabilité du dépôt.

Pour le professionnel, la vérification doit porter sur l'adresse de destination, le mode de transmission et la preuve conservée. La sécurité du compte expéditeur n'élimine pas une difficulté portant sur le canal destinataire. Les outils internes peuvent faciliter cette vérification en maintenant les adresses pertinentes et leur statut. Une erreur de routage est plus facilement évitée si les logiciels distinguent dépôt formel, contact administratif et échange informel, au lieu de présenter tous les courriels d'une juridiction comme interchangeables.

La question ne se limite pas à la transmission. Lorsque les pièces ne sont pas disponibles avant un débat, il faut permettre au juge d'examiner la difficulté au moment où elle peut encore être corrigée. L'arrêt insiste sur la réitération de la demande dès l'ouverture. Pour préparer l'audience, le suivi devrait donc identifier les pièces attendues et les démarches restées sans réponse. Une trace d'envoi ne remplace pas cette vérification de l'accès effectif, surtout lorsque la discussion porte sur une mesure de sûreté.

L'enseignement pour l'inclusion est la lisibilité du parcours juridique. Les exigences de sécurité peuvent être nécessaires, mais elles doivent être expliquées dans la manière dont le service présente ses canaux. La disponibilité technique d'une adresse et la recevabilité d'un acte sont deux propriétés distinctes. Un dispositif bien conçu aide l'utilisateur à choisir le bon chemin et à comprendre ce qui a été accompli, sans confondre message transmis, acte déposé et dossier effectivement accessible.

Notes et références

[1] Inspection générale des finances ; Inspection générale de l'administration ; Inspection générale des affaires sociales. Le déploiement de l'intelligence artificielle dans les administrations publiques — Synthèse et recommandations. Avril 2026 ; publié le 2 juillet 2026. Synthèse, pages imprimées 1-3 ; propositions 5-7 et 9-13, page 4 ; publication IGAS du 2 juillet.

[2] Direction interministérielle du numérique. Intelligence artificielle : une IA utile, humaine et souveraine pour les services publics. 16 juin 2026. Trois piliers ; déploiement des quatre outils ; gouvernance interministérielle et résultat de test de synthèse jusqu'à 16 %.

- [3] Commission européenne. Application des règles IA et nouvelles exigences de transparence le 2 août. 31 juillet 2026. Annonce d'application au 2 août 2026 et obligations pour interactions/contenus ; portée précisée par l'article 50 du règlement.
- [4] Parlement européen ; Conseil de l'Union européenne. Règlement (UE) 2024/1689 sur l'intelligence artificielle — articles 50 et 113. 13 juin 2024 ; application des obligations de transparence le 2 août 2026. Article 50, paragraphes 1-2 et 4-6 : interaction, marquage, déployeur, contrôle éditorial, accessibilité ; article 113 : calendrier.
- [5] Conseil d'État, 10e-9e chambres réunies. Nice — Traitement algorithmique des images devant les écoles, n° 506370. 30 janvier 2026. Points 1, 5-8 et article 1 : détection systématique, insuffisance de L.251-2, risque IA distinct et rejet.
- [6] Équipe data.gouv.fr, Direction interministérielle du numérique. Quelles sont les perspectives de data.gouv.fr pour 2026 ? 18 février 2026. Feuille de route : recherche, score des métadonnées, thématisation et données à accès restreint.
- [7] Cour de cassation, première chambre civile. Archive de presse, suppression et anonymisation — pourvoi n° 25-14.228. 3 juin 2026. Faits 1-5 ; motifs 8-23 et 25-27 ; rejet : sept critères, préjudice, référencement, casier et intérêt du nom.
- [8] Cour de cassation, chambre commerciale financière et économique. Preuve technique pseudonymisée et proportionnalité — pourvoi n° 25-11.499. 17 juin 2026. Faits, motifs 9-12 et rejet ; pseudonymisation, destruction des originaux, absence de contenu de courriels et de fichier nominatif.
- [9] Direction interministérielle du numérique. Plateforme des données de santé : choix d'un cloud souverain. 8 juin 2026 ; choix annoncé le 21 mai. Choix de Scaleway, accompagnement et rôle de décision du GIP ; partie Prochaines étapes : migration et tests.
- [10] Direction interministérielle du numérique. Les règles de la doctrine cloud de l'État. Doctrine institutionnelle ; version consultée le 12 octobre 2026. Règles 4-5 : ressources de sortie et résilience ; règle 10 : adhérences et portabilité.
- [11] Conseil d'État. DARWIN EU — Autorisation de traitements de données de santé, nos 503159 et 504171. 20 mars 2026. Points 3-11 et 13 ; spécialement 4 et 7 sur flux, 10 sur sécurité/risques et durée ; articles 1-3.
- [12] Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Rapport sur l'état de l'internet en France — Présentation de l'édition 2026. 16 juillet 2026. Partie Cloud, données, Data Act, Data Governance Act : recommandation portabilité/interopérabilité et proposition sur frais de transfert.
- [13] Commission européenne. Amende de 550 millions d'euros contre AliExpress pour violation du DSA — Communiqué. 20 juillet 2026 ; mise à jour le 27 juillet. Annonce : risques de produits illicites, dangereux et contrefaits ; mesures correctrices, suivi et astreintes possibles.
- [14] Commission européenne. Constatations préliminaires sur la conception de Facebook et Instagram au titre du DSA — Communiqué. 10 juillet 2026. Constats préliminaires, défilement, lecture automatique, notifications, recommandations et publics vulnérables.
- [15] Conseil d'État, 10e-9e chambres réunies. Tagadamedia — Consentement, droits de la défense et sanction CNIL, n° 492836. 20 mai 2026. Points 7-8 : grief substitué ; 9-11 : formulaires ; 14-15 et articles 1-5 : amende à 50 000 euros et autres dispositions maintenues.
- [16] Agence nationale de la sécurité des systèmes d'information. Cyberattaques : capacité renforcée de réaction dédiée aux services de l'État — REACTIV. 7 septembre 2026. Annonce, compromission de comptes/exfiltration, appui ministériel, mesures contraintes et communication technique centralisée.
- [17] Agence nationale de la sécurité des systèmes d'information. Panorama de la cybermenace 2025 — Présentation. 11 mars 2026. Présentation : 3 586 événements traités, -18 %, comparaison avec pics Jeux 2024 ; exfiltration et équipements exposés.

[18] Agence nationale de la sécurité des systèmes d'information. Cadre réglementaire du Cyber Resilience Act — Présentation française. Page institutionnelle consultée le 12 octobre 2026. Parties Plateforme unique de signalement et calendrier ; fabricants, vulnérabilités exploitées et incidents graves.

[19] Parlement européen ; Conseil de l'Union européenne. Règlement (UE) 2024/2847 sur la cyberrésilience — articles 14 et 71. 23 octobre 2024 ; publié le 20 novembre 2024. Article 14 : fabricants, vulnérabilités activement exploitées, incidents graves et notification par étapes ; article 71 : 11 septembre 2026/11 décembre 2027.

[20] Agence nationale de la sécurité des systèmes d'information. Transition post-quantique : appel à l'action de l'ANSSI et de ses partenaires du G7. 3 septembre 2026. Annonce et recommandations de préparation/migration ; renvoi à la déclaration 2025 et à l'appel 2026.

[21] Conseil d'État. ANEF — Accès normal au téléservice et correction de dysfonctionnements, n° 502860. 5 mai 2026. Points 4-10 : accès/accompagnement/substitution ; 12-17 : blocages ; 46-49 et dispositif : griefs et délais depuis notification.

[22] Cour de cassation, chambre criminelle. Communication pénale et adresse électronique éligible — pourvoi n° 26-81.526. 27 mai 2026. Faits ; motifs 6-19 et rejet : simple lettre, D.591 et destination éligible, réitération dès ouverture du débat.