

La Lettre de XXI Institut – Logiciels, cloud, IA et cybersécurité

Septembre 2026 · XXI Institut

Publication du 17 octobre 2026

Logiciels, interfaces et accès aux marchés

Optima Concept : le droit sur le logiciel ne réserve pas toutes les interfaces compatibles

Le 14 mai 2025, la première chambre civile de la Cour de cassation rejette le pourvoi d'Optima Concept, qui reprochait à des concurrents de commercialiser des interfaces déclenchant ses logiciels de pulvérisation agricole. L'originalité des programmes n'était pas écartée. Le débat portait sur les reproductions provisoires nécessaires à leur exécution par les agriculteurs ayant acquis les équipements et les programmes. L'arrêt dissocie ainsi la protection du code et la maîtrise commerciale de tous les accessoires capables de le faire fonctionner.[1]

Les juges avaient constaté que les acquéreurs disposaient du droit d'utiliser les programmes conformément à leur destination et que la reproduction provisoire intervenait quelle que soit l'interface employée. Aucune stipulation spécifique limitant cet usage n'était justifiée. La Cour approuve le rejet de la contrefaçon dans ces circonstances. Elle admet également le raisonnement écartant l'atteinte au système de traitement de données, compte tenu des droits et de la maîtrise reconnus aux utilisateurs. Le résultat ne repose donc pas sur une prétendue disparition des droits de l'éditeur, mais sur l'examen des actes effectivement accomplis.

Pour un éditeur, la première question contentieuse est de savoir ce que le concurrent reproduit ou modifie. Copier du code, envoyer une commande compatible et provoquer l'exécution normale du programme chez un utilisateur autorisé décrivent des opérations différentes. Une expertise doit les séparer. L'image commerciale d'un produit « fermé » ne démontre ni la matérialité d'une reproduction illicite ni l'absence de droit de l'utilisateur. Inversement, cet arrêt ne constitue pas une permission générale de copier un programme ou de contourner toutes les protections techniques.

La conséquence économique concerne les recettes attendues d'un parc installé. Un fabricant peut avoir prévu de vendre lui-même toutes les interfaces et mises à niveau ; cette prévision n'établit pas l'exclusivité juridique correspondante. Lors d'une acquisition, les revenus du logiciel doivent être distingués de ceux des accessoires, avec les droits qui soutiennent chacun. Pour le concepteur d'une interface concurrente, conserver les analyses de fonctionnement, les conditions d'utilisation et l'origine du code permet de démontrer ce qui a été développé

indépendamment. La compatibilité devient une question de preuve technique et de droits précis, plutôt qu'une qualification commerciale suffisante à elle seule.

Experis : remplacer l'assistant de l'acheteur ne supprime pas les informations déjà connues

Dans sa décision du 3 avril 2026, le Conseil d'État annule une procédure d'achat de support informatique et d'ingénierie lancée par un groupement coordonné par France Télévisions. La directrice générale de l'assistant à maîtrise d'ouvrage était l'épouse du directeur général d'Helpline, candidate retenue. Une première annulation avait conduit l'acheteur à retirer l'assistant, puis à reprendre les négociations avec les mêmes candidats et les mêmes offres initiales. Ce retrait ne suffisait pas à remédier au conflit d'intérêts.[2]

L'élément déterminant était l'accès déjà obtenu aux offres confidentielles des concurrents. L'assistant avait accompagné la première procédure et visité les locaux des soumissionnaires. Lors de cette reprise, l'obligation contractuelle de confidentialité ne permettait pas de rétablir les conditions d'impartialité. Le Conseil d'État impose l'exclusion d'Helpline si l'attribution est poursuivie et annule au stade des candidatures, puisque celles-ci déterminaient le nombre d'opérateurs admis à présenter une offre. La solution répond à cette configuration, non à toute relation entre un conseil et un acteur du marché.

Les achats numériques rendent cette difficulté particulièrement concrète. Une démonstration peut dévoiler une architecture, un prix de service, des méthodes d'exploitation ou l'organisation d'un centre de support. Un intervenant ayant vu ces éléments possède davantage qu'un accès théorique à une salle de consultation. Pour déterminer une mesure corrective, il faut reconstituer les documents reçus, les réunions et le stade auquel une nouvelle compétition peut encore avoir un sens. Changer le nom du conseil sur le dossier ne retire pas la connaissance acquise.

Pour les entreprises de services et les éditeurs, la prévention commence avant la remise des offres. Les missions de conseil, les liens de direction et les accès aux espaces documentaires doivent pouvoir être identifiés. Cette traçabilité protège aussi les candidats contre des accusations insuffisamment établies : un lien allégué et un accès démontré ne se prouvent pas de la même façon. En cas de reprise, le calendrier commercial doit tenir compte du stade réellement annulé. Une procédure recommencée aux candidatures ne correspond pas à une simple prolongation des négociations avec un résultat déjà presque acquis.

Pixels de courriel : une clôture de plainte de 2025 ne dispense pas d'appliquer les recommandations de 2026

Le Conseil d'État avait rejeté, le 31 juillet 2025, le recours contre la clôture d'une plainte visant les pixels et liens traçants d'OVH. La Commission nationale de l'informatique et des libertés (CNIL) avait privilégié un rappel aux obligations et des mesures correctrices ; le juge en admettait la proportionnalité dans le contexte examiné. Cette décision ne délivrait pas une autorisation générale de suivi des courriels. Elle laissait possible une nouvelle intervention si le manquement persistait.[3]

Depuis, la CNIL a publié, le 14 avril 2026, sa recommandation sur les pixels, puis une foire aux questions le 22 juillet. Le document distingue les finalités nécessitant un consentement et des exemptions encadrées. L'optimisation commerciale des campagnes ne se confond pas avec la seule délivrabilité d'un service demandé ou la sécurisation d'une authentification. La recommandation n'est pas un règlement nouveau ; elle explicite les conditions de mise en conformité retenues par l'autorité.[4]

Pour un éditeur de solution d'envoi, la fonction « statistiques » ne doit donc pas être traitée comme une opération unique. Mesurer l'ouverture pour personnaliser une campagne, réduire les envois aux destinataires inactifs et protéger un message d'authentification ont des objectifs différents. Les paramètres et les données conservées doivent permettre de les distinguer. Un même indicateur affiché au client peut provenir d'opérations dont les conditions juridiques ne sont pas identiques. La conception du produit doit rendre cette distinction utilisable, et pas seulement la mentionner dans une politique de confidentialité.

La foire aux questions précise également que les liens traçants ne sont pas directement couverts par la recommandation dédiée aux pixels et que l'agrégation des résultats ne suffit pas à écarter l'article 82. Elle explique comment donner suite au retrait du consentement pour des messages déjà envoyés : les requêtes associées ne doivent plus être exploitées. Pour le fournisseur, cette exigence appelle une capacité technique de désactivation ; une simple modification des futurs modèles de courriel ne règle pas le sort des anciens messages.[5]

Le contrat entre l'expéditeur et le prestataire doit décrire les finalités réellement prises en charge, les instructions et les moyens d'exercer les choix. Une case générale « suivi activé » ne permet pas au client de savoir ce qu'il autorise. La recette du service doit vérifier le comportement après refus ou retrait, avec des essais sur les messages déjà distribués. C'est sur cette fonctionnalité concrète que l'éditeur peut construire une offre de conformité ; la seule référence à la décision OVH ou à une anonymisation annoncée ne permet pas de conclure que tous les usages de suivi sont permis.

Cloud, réversibilité et dépendances

Changer de cloud : distinguer préavis, transfert et récupération des données

Un an après l'application générale du règlement européen sur les données, le 12 septembre 2025, la sortie d'un service cloud ne peut plus être décrite par la seule formule « données restituées à la fin du contrat ». Les articles 23 et 25 du règlement 2023/2854 organisent le changement de fournisseur et son contenu contractuel. Ils distinguent le préavis, la période de transition et la récupération des données. Ces délais remplissent des fonctions différentes ; les réunir dans un délai global peut rendre la migration impraticable.[6]

Le contrat doit prévoir un préavis maximal de deux mois, puis une transition qui, en principe, ne dépasse pas trente jours calendaires. Une impossibilité technique doit être motivée et notifiée dans les quatorze jours ouvrables, avec une autre période n'excédant pas sept mois. Le texte organise aussi une faculté de prolongation à l'initiative du client et une période de récupération

d'au moins trente jours après la transition. Ces mécanismes ne sont ni une promesse que toute migration prend trente jours ni une faculté discrétionnaire pour le fournisseur d'imposer sept mois.

La matière transférable doit être connue avant l'incident ou la résiliation. Données exportables, actifs numériques, formats et informations nécessaires à leur utilisation ne se résument pas à une archive de fichiers. Une base peut être exportée tout en restant inexploitable si les relations entre tables, les identifiants ou les descriptions manquent. Les exclusions destinées à protéger certains éléments internes doivent être explicites et ne pas servir à entraver la sortie. Le travail contractuel commence donc par un inventaire compréhensible par les équipes qui réaliseront le transfert.

L'article 30 différencie également les services d'infrastructure et les autres services. L'équivalence fonctionnelle n'impose pas de reproduire à l'identique toute une application chez le nouveau fournisseur ; le règlement ne commande pas de créer de nouvelles technologies ni de transférer tous les secrets du fournisseur. Pour le client, il reste nécessaire de vérifier les fonctions dont il a réellement besoin. Un export réussi ne prouve pas que les traitements, les droits d'accès et les sauvegardes fonctionneront dans l'environnement de destination.

Une sortie se prépare ainsi comme une opération avec des responsabilités partagées : qui extrait, qui valide l'intégrité, qui conserve le service pendant la bascule et qui autorise l'effacement final ? La coopération du fournisseur de destination compte autant que l'assistance du fournisseur quitté. Les tests doivent porter sur un jeu de données représentatif et sur les dépendances qui empêcheraient la reprise. La qualité d'une clause se mesure à sa capacité d'organiser ces opérations, et pas à la seule présence du mot « réversibilité ».

Frais de sortie du cloud : septembre 2026 reste une période de transition tarifaire

L'article 29 du règlement sur les données fixe au 12 janvier 2027 la suppression des frais de changement de fournisseur. En septembre 2026, il admet encore des frais réduits, plafonnés aux coûts directement liés au processus concerné. Présenter la suppression future comme une gratuité déjà générale fausse la comparaison entre offres. À l'inverse, le maintien temporaire d'une facturation n'autorise pas un montant forfaitaire sans rapport avec les coûts que le texte permet de retenir.[6]

Le règlement distingue les frais de changement, les frais de service ordinaires et les pénalités de résiliation anticipée à présenter avant la conclusion du contrat. Une ligne commerciale « sortie gratuite » n'explique donc pas à elle seule la totalité du coût supporté. Le client doit pouvoir isoler ce qu'il paie pour transférer ses données, ce qu'il paie pour continuer le service et ce qui correspond éventuellement à un engagement de durée. Cette décomposition permet de discuter une facture sans traiter tous les montants comme une catégorie juridique unique.

Le régime particulier des services conçus sur mesure mérite lui aussi une lecture précise. L'article 31 prévoit des exceptions pour certaines obligations, sous des conditions relatives aux caractéristiques principales, au développement spécifique et à l'absence d'offre à grande échelle dans le catalogue. Il n'écarte pas indistinctement tout le chapitre sur la sortie. Ajouter

quelques paramétrages à une offre standard n'établit pas, par lui-même, qu'elle relève de cette exception. Le fournisseur doit également informer le client avant le contrat des obligations qui ne s'appliqueront pas.

Pour une entreprise cloud, la préparation de janvier 2027 concerne la structure de prix et l'organisation du service. Les coûts de migration ne disparaissent pas matériellement parce qu'un frais ne pourra plus être facturé comme auparavant. Il faut prévoir les capacités de support, les outils d'export et les moyens de documenter les tâches. Pour l'acheteur, le prix de la sortie doit être comparé aux moyens internes et au travail du prestataire entrant. Supprimer une ligne de facture ne suffit pas à rendre une architecture portable ; la décision économique doit regarder l'ensemble de l'opération sans confondre coût technique et frais juridiquement exigibles.

DARWIN EU : héberger en France et répondre aux demandes étrangères sont deux questions distinctes

Le 20 mars 2026, le Conseil d'État rejette les recours contre l'autorisation donnée à l'Agence européenne des médicaments pour des études DARWIN EU. Les données de santé extraites du système national étaient hébergées en France par Microsoft Ireland, via la Plateforme des données de santé. Le juge prend en compte les mesures de protection du projet et sa durée limitée à trois ans. Il ne certifie pas la conformité générale de tous les services de ce groupe pour toutes les administrations.[7]

La décision distingue les données de santé et les données techniques de connexion. L'autorisation n'a pas pour objet d'autoriser un transfert de santé vers les États-Unis sur le fondement de la décision d'adéquation. Pour les données techniques d'usage, le juge examine les garanties contractuelles. Il reconnaît par ailleurs que le risque d'une demande d'accès étrangère aux données de santé ne peut être totalement exclu. L'hébergement physique et l'exposition juridique ne décrivent donc pas le même risque.

Le Conseil d'État retient notamment la pseudonymisation, la limitation de conservation et les contrôles des extractions et des traces. La certification d'hébergeur de données de santé participe aux garanties examinées, alors que Microsoft Ireland ne peut bénéficier de SecNumCloud dans les circonstances relevées. Ces éléments ne sont pas des labels interchangeables. Une entreprise qui répond à une consultation doit pouvoir expliquer exactement quelle garantie son offre possède et ce qu'elle ne couvre pas, plutôt que présenter une certification comme substitut automatique à toutes les autres exigences.

Pour l'analyse d'une offre cloud, trois inventaires sont utiles : les données stockées, les accès d'administration et les demandes auxquelles l'opérateur peut être soumis. Les conditions de sous-traitance doivent correspondre à ces flux. Une carte des centres de données ne montre pas nécessairement où se trouvent les personnes chargées du support, ni quelles traces sont accessibles. Le contrat et l'architecture doivent permettre d'identifier ces situations avant de discuter leur acceptabilité pour le traitement envisagé.

L'arrêt invite aussi à dater l'analyse. Le juge examinait la délibération de février 2025 et relevait l'absence, à cette date, du décret nécessaire à l'invocabilité de certaines dispositions de la loi de 2024. Cette constatation ne permet pas d'affirmer que les mêmes conditions restent inchangées pour une décision prise plus tard. Pour le fournisseur, la valeur du précédent tient à la méthode d'examen des garanties du projet ; elle ne dispense pas de vérifier le droit et les exigences de l'acheteur à la date du nouveau contrat.

CADA : l'annonce d'un cadre européen ne constitue pas encore un classement des offres cloud

Le 3 juin 2026, la Commission européenne a présenté sa proposition de Cloud and AI Development Act, COM(2026) 502. La présentation officielle articule trois objectifs : recherche et innovation, développement des capacités de centres de données et autonomie. Elle annonce un cadre commun d'évaluation de la souveraineté du cloud et de l'IA, accompagné d'un mécanisme d'adoption par le secteur public. Il s'agit de la présentation d'une proposition, et non d'une certification déjà attribuée aux prestataires.[8]

Pour le marché, l'intérêt du projet est de rendre comparables des qualités aujourd'hui souvent regroupées sous le mot « souverain ». Localisation des calculs, maîtrise de l'opérateur, dépendance aux composants et accès aux données ne se mesurent pourtant pas avec un seul indicateur. Un service peut être exploité en Europe et dépendre d'une technologie extérieure ; un fournisseur européen peut lui-même sous-traiter une partie des opérations. Une information utile à l'acheteur doit décrire ces dépendances séparément.

Les éditeurs et fournisseurs cloud ont donc intérêt à constituer des preuves sur leur offre réelle : entités contractantes, lieux d'exécution, fonctions administrées par des tiers, continuité et conditions de changement. Ces pièces peuvent servir à plusieurs exigences d'achat sans préjuger du classement qui résultera d'une législation future. Une promesse commerciale fondée sur une catégorie encore en discussion expose au risque de devoir modifier l'offre ou son prix lorsque les critères seront arrêtés.

Le développement des centres de données pose une autre question : une capacité annoncée n'est pas une ressource déjà disponible pour un client. Calendrier de mise en service, accès à l'énergie et type de service livré déterminent ce qui pourra réellement être acheté. Les pouvoirs publics doivent pouvoir distinguer soutien à une infrastructure et acquisition d'un service exploitable ; les entreprises, une perspective d'investissement et un engagement contractuel ferme. Ce sont ces différences qui permettent de discuter les effets industriels du projet sans convertir ses objectifs en obligations déjà acquises.

Intelligence artificielle, usages et explications

Règlement IA : le report de certaines exigences ne suspend pas tous les autres droits

Le règlement 2026/1744 du 8 juillet 2026 a modifié le calendrier du règlement européen sur l'intelligence artificielle. Pour les sections 1 à 3 du chapitre III, sous l'exception prévue pour l'article 6, paragraphe 5, il distingue le 2 décembre 2027 pour les systèmes classés à haut risque par l'article 6, paragraphe 2, et l'annexe III, et le 2 août 2028 pour ceux relevant de l'article 6, paragraphe 1, et de l'annexe I. Ces renvois sont plus précis que la formule « toute l'IA est reportée ».[9]

Le même texte prévoit des transitions particulières. Pour certains systèmes générant des contenus de synthèse mis sur le marché avant le 2 août 2026, il fixe au 2 décembre 2026 la mise en conformité avec l'article 50, paragraphe 2. Cette disposition ne reporte pas automatiquement toutes les obligations de transparence pour tous les acteurs. Les contrats doivent distinguer les systèmes, la date de mise sur le marché, le rôle du fournisseur et l'obligation considérée. Un calendrier commercial unique pour l'ensemble d'une gamme peut masquer des situations différentes.

Pour un intégrateur, l'exercice commence par le cas d'usage. Un même modèle peut alimenter une aide rédactionnelle, une application de sélection ou un composant de produit ; la catégorie du modèle ne suffit pas à qualifier tous les systèmes construits avec lui. La description du produit vendu doit permettre de comprendre la finalité, les données et la place du résultat dans la décision. Les documents remis par le fournisseur du modèle ne décrivent pas nécessairement tout ce que l'intégrateur ajoute ou promet au client.

Le report peut modifier la planification des travaux de conformité, mais il ne transforme pas les données collectées en ressources librement utilisables. Les droits des personnes, la propriété intellectuelle, les engagements de confidentialité et les règles de l'activité conservent leurs objets propres. Une clause affirmant que « le produit n'est pas encore soumis à l'IA Act » ne répond pas à ces questions. Elle peut aussi devenir rapidement inexacte si l'entreprise fait évoluer la fonction ou la population concernée.

Une préparation utile consiste à rattacher chaque exigence à un produit et à un responsable capable d'en produire la preuve. Les essais, les versions et les incidents doivent rester traçables pendant le développement. Cela permet de différer un livrable lorsque le texte le permet, sans perdre les informations nécessaires à sa réalisation ultérieure. Le gain de délai ne devient un gain industriel que si l'entreprise sait quels travaux elle déplace et quelles décisions elle doit déjà pouvoir justifier.

Nice : une caméra autorisée ne donne pas par elle-même le droit d'analyser toutes ses images

Le 30 janvier 2026, le Conseil d'État rejette le recours de Nice contre la position de la CNIL sur un traitement nommé « zone d'intrusion entrées des écoles ». Le logiciel détectait automatiquement des véhicules stationnant irrégulièrement devant les écoles pendant leur ouverture, puis alertait la police municipale. Le juge considère que les dispositions autorisant la vidéoprotection ne peuvent, dans leur silence, autoriser cette analyse systématique et automatisée. Aucune autre disposition ne fondait le traitement examiné.[10]

La décision ajoute que la solution demeure même en supposant que le système ne soit pas une IA à haut risque. L'autorisation de l'usage ne se déduit donc pas de son classement dans le règlement européen. Le droit de capter une image, le droit de l'analyser automatiquement et les obligations pesant sur le produit répondent à des questions distinctes. Pour un fournisseur, l'existence d'une caméra légalement installée ne suffit pas à établir la licéité de toutes les fonctions ajoutées après son installation.

Cette séparation doit intervenir avant le pilote commercial. Une expérimentation peut déjà traiter des personnes, analyser leurs comportements ou déclencher une intervention. Le fait de présenter une fonction comme une simple assistance ne change pas matériellement les opérations effectuées. La description technique doit préciser ce qui est détecté, avec quelle continuité, quels destinataires et quelle action attendue. Ce sont ces faits qui permettent ensuite de rechercher le régime applicable, et pas l'inverse.

Le contrat ne peut pas combler à lui seul l'absence de fondement légal du traitement. Il peut en revanche organiser les responsabilités de vérification, les paramètres autorisés et les conditions de suspension lorsqu'un usage change. Pour l'éditeur qui vend à plusieurs clients publics, il est préférable de distinguer la capacité technique du produit et les configurations dont l'utilisation est juridiquement possible. Une bibliothèque de fonctionnalités commercialement disponibles ne constitue pas une liste d'usages automatiquement autorisés pour chaque acheteur.

Dun & Bradstreet : expliquer un score exige davantage que livrer une formule ou une notice générale

Dans l'arrêt C-203/22 du 27 février 2025, la Cour de justice précise le droit d'obtenir des informations utiles sur la logique d'une décision automatisée. L'affaire concernait un profil de solvabilité associé au refus d'un contrat de téléphonie. La réponse doit expliquer, de manière intelligible, la procédure et les principes concrètement appliqués aux données de la personne pour produire le résultat. Une description générale du produit ne répond donc pas nécessairement à la demande individuelle.[11]

La Cour ne prescrit pas la remise systématique de l'algorithme complet. Une formule complexe ou le détail de toutes les étapes peut rester incompréhensible. Elle envisage notamment une explication de la manière dont une variation des données aurait conduit à un résultat différent. Elle traite aussi le secret des affaires : celui-ci ne justifie pas un refus absolu, les informations

prétendument protégées devant pouvoir être communiquées à l'autorité ou au juge compétent pour une mise en balance. Le litige individuel reste à résoudre par la juridiction nationale.

Pour le fournisseur de scoring, cela conduit à distinguer trois objets : le fonctionnement général du modèle, les données d'une personne et le résultat effectivement produit à une date donnée. Un modèle mis à jour après le refus peut donner une autre réponse ; sa documentation courante ne reconstitue pas nécessairement la décision initiale. Les systèmes doivent donc conserver les éléments permettant de retrouver la version et les données utilisées. Sans cette traçabilité, le client peut acheter un service performant tout en restant incapable de répondre à une demande d'explication.

La répartition contractuelle des tâches est déterminante. L'entreprise qui prend la décision ne doit pas promettre une explication que son prestataire refuse ou ne sait pas produire. Le fournisseur doit, de son côté, identifier les informations qui peuvent être rendues compréhensibles sans révéler inutilement ses actifs. Préparer des niveaux de communication et un circuit d'examen des informations sensibles est plus utile qu'une opposition générale entre transparence et secret. L'explication doit porter sur le résultat de la personne, tout en permettant le contrôle des éléments dont la divulgation est discutée.

Cybersécurité, incidents et preuve des corrections

11 septembre 2026 : les fabricants doivent organiser les notifications de cyberrésilience avant le régime général

Depuis le 11 septembre 2026, l'article 14 du règlement 2024/2847 sur la cyberrésilience s'applique aux fabricants pour les vulnérabilités activement exploitées et les incidents graves affectant la sécurité des produits comportant des éléments numériques. L'article 71 fixe l'application générale au 11 décembre 2027, mais réserve cette échéance anticipée. Un éditeur ne peut donc pas conclure de la date de 2027 qu'aucun processus de signalement n'est nécessaire en septembre.[12]

Les événements doivent être qualifiés. Une vulnérabilité découverte ne signifie pas toujours exploitation active ; un incident n'est pas nécessairement grave au sens de cet article. Pour les cas concernés, une alerte précoce est attendue sans retard injustifié, au plus tard vingt-quatre heures après connaissance, puis une notification au plus tard à soixante-douze heures. Le rapport final suit deux calendriers : quatorze jours après disponibilité d'une correction ou atténuation pour la vulnérabilité, et un mois après la notification pour l'incident grave. Les destinataires comprennent le centre de réponse désigné comme coordinateur et l'Agence de l'Union européenne pour la cybersécurité (ENISA), via la plateforme prévue.

La qualification de fabricant doit elle aussi être vérifiée. Le règlement vise des produits logiciels ou matériels et certaines solutions de traitement à distance ; tous les services numériques ne deviennent pas des produits identiques parce qu'ils sont accessibles en ligne. L'éditeur, le distributeur et le prestataire de surveillance peuvent participer au même incident sans porter la

même obligation. Les contrats doivent permettre de savoir qui reçoit l'alerte technique, qui apprécie le signalement et qui dispose des informations sur les versions affectées.

La procédure doit fonctionner pendant que l'analyse reste incomplète. Attendre une attribution certaine de l'attaque peut empêcher de respecter les premiers délais. Le dossier doit distinguer faits connus, hypothèses et recherches en cours, avec une chronologie des décisions. L'alerte au client ne remplace pas nécessairement la notification réglementaire ; le dépôt sur une plateforme ne suffit pas à organiser l'installation du correctif. Le prestataire doit préciser sa permanence, les destinataires habilités et les journaux conservés. Même si le client conserve la qualification juridique, il doit recevoir les informations techniques nécessaires que seul le prestataire détient. La répartition contractuelle des tâches doit permettre cette coopération dans les délais.

Panorama ENISA du 22 septembre : mesurer les dépendances plutôt que convertir des incidents observés en probabilités

L'Agence de l'Union européenne pour la cybersécurité, l'ENISA, a publié le 22 septembre 2026 son nouveau panorama des menaces. Les observations portent sur janvier à décembre 2025, et non sur tous les incidents de 2026. La méthode recense 8 257 incidents à partir de sources ouvertes et d'informations partagées, avec une couverture explicitement incomplète. Le changement de période crée également un chevauchement de six mois avec l'édition précédente. Les deux totaux ne constituent donc pas une série annuelle directement comparable.[13]

Les premières sections distinguent la fréquence des événements observés et leurs conséquences. Les attaques par déni de service occupent une place importante dans le corpus, sans que cela signifie qu'elles produisent toujours le dommage le plus lourd pour une entreprise. Le rapport met aussi en évidence les dépendances envers les fournisseurs, les services tiers et les environnements cloud. Il fournit ainsi une lecture des chemins de propagation, plutôt qu'une probabilité individuelle de sinistre applicable uniformément à chaque client.

Pour un prestataire, la première traduction est la cartographie des fonctions communes. Plusieurs sauvegardes peuvent dépendre du même compte d'administration ; deux applications différentes, du même composant ou de la même infrastructure d'identité. Compter les fournisseurs ne suffit pas à mesurer cette concentration. Le contrat et les exercices de reprise doivent permettre de vérifier ce qui reste disponible lorsque cette dépendance particulière est atteinte. Une architecture apparemment répartie peut conserver un point d'arrêt unique.

L'utilisation des statistiques dans une offre commerciale demande la même précision. Le nombre de cas connus dépend des sources, de la visibilité des attaques et de leur publication. Il ne permet pas de promettre un taux de protection ou d'établir que les incidents non observés sont absents. L'éditeur peut s'appuyer sur les scénarios documentés pour construire des essais ; il doit distinguer cette sélection de la preuve que son produit les détecte effectivement. Le protocole, le périmètre et les résultats des tests constituent alors les pièces pertinentes pour le client.

Pour l'acheteur, le panorama aide enfin à hiérarchiser les questions à poser : capacité de détection, confinement, restauration et coopération avec les tiers. Ces capacités ne se compensent pas automatiquement. Une intervention rapide qui détruit les traces peut compliquer l'analyse ; une conservation parfaite qui retarde la reprise peut prolonger l'arrêt. Les exercices doivent éprouver ces arbitrages sur les services essentiels à l'activité. L'utilité du rapport tient à ce travail de scénarios documentés, pas à l'affichage isolé d'un pourcentage de menace.

Lydia : corriger le canal de collecte peut compter davantage qu'un rappel abstrait à la sécurité

Le 17 juin 2026, le Conseil d'État rejette le recours contre la clôture d'une plainte visant Lydia Solutions. Pour restituer un solde de compte, la société avait demandé, par courriel ordinaire, une pièce d'identité, un autoportrait tenant cette pièce et un relevé bancaire. Après intervention de la CNIL, elle avait reconnu l'insuffisance du canal et proposé la messagerie sécurisée de son application. Le juge admet la clôture au regard de cette réponse ; il ne valide pas la méthode de transmission initiale.[14]

Le dossier illustre la différence entre justifier une demande et protéger sa collecte. Même lorsqu'une entreprise estime nécessaire de vérifier une identité, elle doit examiner le moyen par lequel les documents seront transmis. Le support client peut créer un risque distinct du service principal. Une application protégée ne rend pas sûr un échange parallèle qui fait sortir des documents de ses circuits habituels. L'analyse doit donc suivre le parcours réel des pièces, et pas seulement les fonctions présentées dans le dossier commercial.

La correction doit être utilisable par les personnes et les équipes. Proposer un canal sécurisé sans prévoir les droits d'accès, la conservation et le traitement des demandes peut déplacer le problème. Pour un éditeur de solution de support, le produit doit permettre d'éviter l'envoi vers les boîtes ordinaires, d'orienter les utilisateurs et de tracer les changements. Les responsables doivent aussi pouvoir identifier les anciennes pratiques qui continueraient malgré une nouvelle consigne.

Sur le contentieux, la décision concerne les suites données par la CNIL à la plainte et le contrôle de son appréciation dans les circonstances examinées. Elle ne tranche pas toutes les difficultés contractuelles évoquées entre le client et l'entreprise. Pour apprécier la portée économique d'un tel résultat, il faut donc conserver l'objet du recours : absence d'annulation de la clôture ne signifie ni absence de manquement initial ni règlement de tous les différends. La preuve d'une correction concrète reste une ressource utile ; elle ne constitue pas une immunité pour toute la relation de service.

Notes et références

[1] Cour de cassation, première chambre civile. Arrêt du 14 mai 2025, n° 23-20.217 — Optima Concept. 14 mai 2025. Paragraphes 1-4, 7-13, 15-18 ; dispositif.

[2] Conseil d'État. Décision du 3 avril 2026, n° 510005 — Experis France. 3 avril 2026. Points 1-3, 7-12 ; dispositif, articles 1-3.

[3] Conseil d'État. Décision du 31 juillet 2025, nos 490190 et 493614 — pixels et liens OVH. 31 juillet 2025. Points 2, 5, 8-14 et dispositif.

[4] CNIL. Recommandation relative aux pixels de suivi dans les courriers électroniques. Délibération n° 2026-042 du 12 mars 2026 ; publication le 14 avril. Pages imprimées 2-6 : portée, acteurs, finalités, consentement et exemptions.

[5] CNIL. Questions-réponses — recommandation relative aux pixels dans les courriers électroniques. 22 juillet 2026. Questions 1, 18 et 22 ; également 25-26 pour le contexte temporel.

[6] Parlement européen et Conseil. Règlement (UE) 2023/2854 — règlement sur les données. 13 décembre 2023. Articles 23, 25, 27, 29-31 et 50 : changement de fournisseur, frais et calendrier.

[7] Conseil d'État. Décision du 20 mars 2026, nos 503159 et 504171 — DARWIN EU. 20 mars 2026. Points 3-13 et dispositif, article 2.

[8] Commission européenne — DG CONNECT. Proposal for the Cloud and AI Development Act (CADA). 3 juin 2026 ; page mise à jour le 8 juin. Présentation, trois objectifs et liste des documents COM(2026) 502.

[9] Parlement européen et Conseil. Règlement (UE) 2026/1744 du 8 juillet 2026 — omnibus numérique sur l'IA. 8 juillet 2026 ; JO du 24 juillet. Article 1, points 39 et 40 : articles 111 et 113 modifiés ; article 4.

[10] Conseil d'État. Décision du 30 janvier 2026, n° 506370 — Commune de Nice. 30 janvier 2026. Points 1, 5-8 et dispositif.

[11] Cour de justice de l'Union européenne, première chambre. Arrêt du 27 février 2025, C-203/22 — Dun & Bradstreet Austria. 27 février 2025. Points 58-66, 67-76 et dispositif.

[12] Parlement européen et Conseil. Règlement (UE) 2024/2847 — cyberrésilience. 23 octobre 2024. Articles 2-3, 14, 69 et 71 ; notamment article 14, paragraphes 1-8.

[13] ENISA — Agence de l'Union européenne pour la cybersécurité. ENISA Threat Landscape 2026. 22 septembre 2026. Pages imprimées 7-12 : synthèse, méthode, premières tendances ; spécialement pages 9-10.

[14] Conseil d'État. Décision du 17 juin 2026, n° 509593 — plainte Lydia Solutions. 17 juin 2026. Points 1, 4-8 et dispositif.