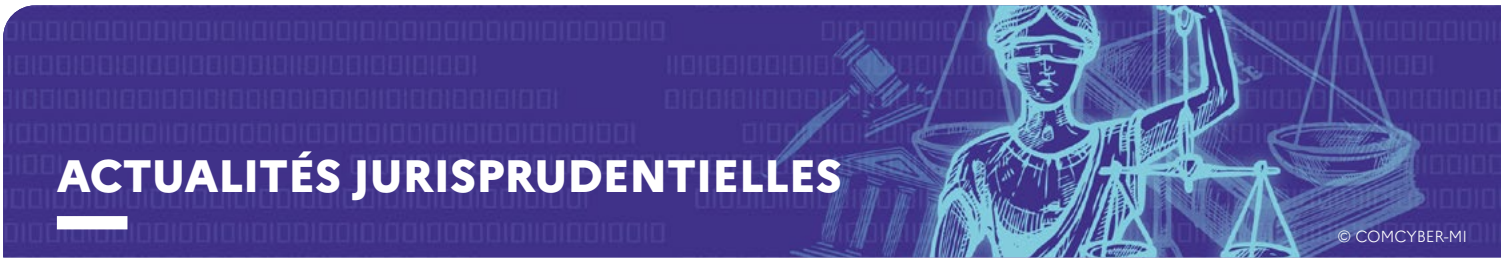
MINISTÈRE
DE L'INTÉRIEUR
*Liberté
Égalité
Fraternité*

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

VEILLE JURIDIQUE 03



Intelligence artificielle et vidéosurveillance : illégalité des traitements algorithmiques en l'absence de dispositions législatives l'autorisant

Cour administrative d'appel de Nantes, 4e chambre, 6 mars 2026, n° 24NT01809

Cette décision porte sur l'adaptation à des développements d'intelligence artificielle de l'architecture d'un parc de caméras de vidéosurveillance.

En l'espèce, le conseil municipal de Vannes a pris la décision d'étendre son réseau de vidéo protection et de mettre en œuvre des systèmes automatisés de traitement des données, de lecture automatisée de plaques d'immatriculation et d'intelligence artificielle.

Un individu demande l'annulation de cette décision d'extension pour les motifs suivants : insuffisance de la note explicative de synthèse, défaut d'autorisation préfectorale et absence d'analyse d'impact relative à la protection des données personnelles.

En l'occurrence, ces développements consistaient à permettre, notamment, un classement des piétons circulant dans les zones définies et très fréquentées selon des typologies tenant à leur taille, leur forme, leur habillement, leurs équipements ou encore leur comportement physique.

L'apport déterminant de cette décision repose sur la question de la légalité de l'analyse systématique et automatisée des images collectées dans des espaces publics au moyen de systèmes de traitement algorithmique.

La Cour administrative d'appel de Nantes juge que les dispositions de l'article L. 251-2 du Code de la sécurité intérieure, si elles permettent la mise en œuvre de systèmes de vidéo protection, ne sauraient, dans leur silence, être interprétées comme autorisant la mise en œuvre de traitements algorithmiques permettant une analyse systématique et automatisée des images collectées dans les espaces publics. Dans l'état actuel du droit, aucune disposition législative n'autorise de tels traitements. L'article L. 251-2 du Code de la sécurité intérieure ne permettant que la vidéo protection « classique ». Toute extension fonctionnelle substantielle d'un réseau de vidéo protection par adjonction d'algorithmes d'analyse requiert une intervention expresse du législateur.

La proportionnalité d'un traitement algorithmique d'images publiques aux finalités poursuivies de prévention des atteintes aux personnes et aux biens ne suffit pas à fonder sa légalité.

Déchiffrement de données : mise au clair dans un cadre juridique et principe du contradictoire

Cour de cassation, chambre criminelle, 1er avril 2026, n° 25-82.181

Dans cette décision, la Cour de cassation confirme la validité du déchiffrement de messageries par des techniques classifiées dans une enquête pénale.

Cette décision s'inscrit dans le contentieux relatif à l'exploitation judiciaire de réseaux de communications chiffrées par des services d'enquête. En l'espèce, une information a été ouverte des chefs, notamment, d'infractions criminelles et correctionnelles à la législation sur les stupéfiants et association de malfaiteurs. Condamné à une peine de neuf ans de prison en appel, le prévenu conteste le versement aux pièces de la procédure de données déchiffrées par des moyens couverts par le secret de la défense nationale.

La question de principe soulevée par l'affaire interroge les droits de la défense. Le recours par les autorités judiciaires aux techniques de déchiffrement de données à travers des moyens couverts par le secret de la Défense nationale est-il conforme au droit à un procès équitable ?

La Cour de cassation rejette le pourvoi et considère que le recours à des techniques de déchiffrement et l'absence de transparence sur leurs modalités précises ne sont pas, en

soi, causes de nullité. Elle s'appuie sur une jurisprudence de la Cour européenne des droits de l'homme (CEDH, 23 mai 2017, Van Wesenbeeck c. Belgique), qui précise que le droit à une divulgation de preuves pertinentes n'est pas absolu et qu'il peut être nécessaire, dans certains cas, de dissimuler certaines preuves de façon à sauvegarder un intérêt public important.

Le recours à des moyens de l'État soumis au secret de la défense nationale pour accéder en clair à des données chiffrées est prévu par la loi, doit être autorisé par un magistrat ou une juridiction qui en contrôle la mise en œuvre et peut ordonner à tout moment son interruption. Ne sont soustraits au contradictoire que les seules techniques utilisées pour les déchiffrer.

La fouille acceptée entraîne l'accès aux données

Cour de cassation, chambre criminelle, 19 mai 2026, n° 25-87.563

Cette décision précise que l'accord donné pour la perquisition et la fouille des affaires personnelles autorise les enquêteurs à exploiter le contenu des téléphones portables saisis sans nécessiter un consentement séparé ou spécifique au support numérique.

En l'espèce, un individu a été mis en examen des chefs d'infractions à la législation sur les produits stupéfiants, blanchiment et association de malfaiteurs. Lors de l'enquête préliminaire, l'intéressé a donné son assentiment à la fouille de ses affaires personnelles et de son sac à dos et à la saisie de tout objet utile à la manifestation de la vérité que celles-ci pourraient contenir.

Un premier téléphone a été découvert, pour lequel l'intéressé a volontairement communiqué aux enquêteurs le code de déverrouillage, puis un second. Il a déclaré que le second appareil découvert n'était pas en fonction et n'avait pas du numéro. Les enquêteurs ont tout de même procédé à son exploitation.

La régularité de cette exploitation est au cœur du contentieux. Se posait la question de la régularité de l'exploitation du second téléphone portable du mis en examen.

La Cour de cassation rejette le pourvoi et considère qu'en application de l'article 76 du Code de procédure pénale, en donnant régulièrement son assentiment à la fouille de ses effets personnels et à la saisie de tout objet utile à la manifestation de la vérité que ceux-ci pourraient contenir, une personne consent à l'exploitation des données à caractère personnel contenues dans les téléphones saisis à cette occasion.

Elle ajoute que l'autorisation préalable d'un juge ou d'une autorité administrative indépendante requise par la Cour de justice de l'Union européenne pour l'exploitation, dans le cadre d'une enquête pénale, des données personnelles contenues dans un téléphone (CJUE, 4 octobre 2024, C-548/21) ne s'impose qu'à défaut du consentement de la personne concernée à cette exploitation.

Revenge porn : précisions sur l'objet du consentement

Cour de cassation, chambre criminelle, 23 juin 2026, F-B, n° 25-82.188

Dans cette décision, la Cour de cassation précise la portée de l'article 226-1 2° du Code pénal. L'envoi volontaire d'une image ne vaut pas autorisation d'en disposer.

En l'espèce, un individu est poursuivi pour atteinte à l'intimité de la vie privée d'autrui et conservation et diffusion auprès du public ou d'un tiers d'enregistrements ou de documents issus de ces infractions. La victime s'était elle-même filmée et avait transmis les vidéos via des messages éphémères (visionnage unique garantissant une suppression automatique plusieurs secondes après leur consultation). Le destinataire a copié ces fichiers vidéos sur son téléphone et son ordinateur, à l'insu de leur auteur, sans l'en informer.

Une telle copie constitue-t-elle un enregistrement sans consentement au sens de l'article 226-1 2° du Code pénal ?

La Cour de cassation censure le raisonnement de la Cour d'appel, qui a raisonné au nom de l'interprétation stricte de la loi pénale. Elle juge que le prévenu avait procédé à l'enregistrement des images litigieuses à l'insu de la partie civile, cette dernière ne lui ayant transmis que pour un visionnage unique suivi d'une suppression automatique. Il s'en déduisait ainsi son absence de consentement auxdites opérations d'enregistrement.

Géolocalisation : mise en place d'un dispositif technique de géolocalisation dans des parties communes

Cour de cassation, chambre criminelle, 30 juin 2026, 25-88.208

Dans cette décision, la Cour de cassation admet la légalité d'un dispositif technique de géolocalisation mis en place sur le véhicule d'un suspect, situé dans le parking privé d'une résidence.

En l'espèce, un individu est poursuivi des chefs d'infraction à la législation sur les stupéfiants et association de malfaiteurs. Au cours de leur enquête, des fonctionnaires de police ont procédé à la mise en place d'un dispositif technique de géolocalisation en temps réel du véhicule du mis en cause, situé dans l'enceinte du parking privé de sa résidence. Une mise en place effectuée en dehors des heures prévues par l'article 59 du Code de procédure pénale (3h30 du matin). L'intéressé faisait valoir qu'il ne résultait pas des pièces de la procédure que les fonctionnaires de police disposaient d'une autorisation expresse et spéciale.

Se posait en particulier la question de la régularité de la mise en place du dispositif de géolocalisation installé, pour lequel l'intéressé a présenté une requête en annulation de pièces de la procédure.

La Cour de cassation admet l'accès des enquêteurs aux parties communes de la résidence du mis en cause au visa de l'article L. 272-1 du Code de la sécurité intérieure et émet des conditions strictes. Cet article dispose que les propriétaires ou les exploitants d'immeubles à usage d'habitation

ou leurs représentants s'assurent que les services de police et de gendarmerie nationales sont en mesure d'accéder aux parties communes de ces immeubles aux fins d'intervention.

La plus haute juridiction considère ainsi que les fonctionnaires de police ont pénétré dans ces lieux dans l'exercice d'une mission de police judiciaire et n'ont réalisé d'autres actes que ceux que la loi les autorisait à accomplir à cette fin. Le parking commun aux occupants de l'immeuble relevant de ces parties communes, aucune autorisation spéciale prévue à l'article 230-34 du Code de procédure pénale n'était donc requise.

Collecte de données sensibles biométriques, oui mais à condition d'une « nécessité absolue »

Cour de justice de l'Union européenne, 19 mars 2026, C-371/24

Dans cette décision, la Cour de justice de l'Union européenne clarifie les exigences imposées aux autorités nationales lorsqu'elles procèdent à la collecte de données biométriques à des fins d'enquêtes pénales.

En l'espèce, un militant écologiste, interpellé pour des faits d'organisation de manifestation non déclarée et rébellion, refuse notamment, lors de sa garde à vue, de se soumettre à des relevés signalétiques (prise d'empreintes digitales et photographies). Il sera finalement condamné par le tribunal correctionnel de Paris à une amende d'un montant de 300 euros pour refus de la collecte de ses données biométriques. Contestant ladite peine, il interjette appel de ce jugement devant la Cour d'appel de Paris qui sursoit à statuer, et pose trois questions préjudicielles à la Cour de justice de l'Union européenne. **Cette dernière doit se prononcer sur la compatibilité de l'article 55-1 du Code de procédure avec les dispositions prévues par la directive « Police-Justice ».**

Plus précisément, la juridiction de renvoi **demande en substance si le droit de l'Union permet aux autorités nationales de collecter systématiquement les empreintes digitales et la photographie de toute personne soupçonnée d'une infraction pénale, sans devoir justifier cette mesure au cas par cas.**

Dans sa décision, la Cour de justice dit pour droit que l'autorité nationale compétente ne peut collecter les données biométriques qu'en cas de « nécessité absolue ». La finalité justifiant cette opération de traitement devant être définie et vérifiée individuellement par l'autorité compétente par le biais d'une motivation que l'article 55-1 du Code de procédure pénale n'exige pas à ce jour. Il doit s'agir d'une motivation claire, même succincte, permettant à la personne concernée de comprendre les raisons de la mesure et d'exercer son droit de recours si elle le désire.

Une réglementation nationale, qui rendrait ces relevés systématiques, sans que l'autorité répressive compétente puisse apprécier leur nécessité au cas par cas, serait contraire au droit de l'Union puisqu'elle aboutirait à une collecte indifférenciée et généralisée.



Procédure pénale – Accès aux données numériques dans les enquêtes pénales : lignes directrices pour les parquets

La circulaire du 13 avril 2026 (n° JUSD2605231C) porte sur l'accès aux données détenues par les fournisseurs de services et de messageries électroniques dans le cadre des enquêtes pénales.

Elle insiste, notamment, sur les points suivants. Pour l'accès aux données de contenu, la circulaire prévoit la possibilité de recourir aux techniques spéciales d'enquête prévues par le Code de procédure pénale. Elle indique que les autorités judiciaires peuvent solliciter une remise volontaire des données, notamment via des plateformes dédiées.

En matière de coopération internationale et d'appui des services spécialisés, le bureau de l'entraide pénale internationale (DACG) doit être contacté pour identifier les bons canaux conventionnels et signaler l'urgence. Les services spécialisés comme l'Office anti-cybercriminalité (OFAC) et l'Unité nationale cyber (UNC) sont identifiés comme points d'appui techniques pour préciser toutes les informations utiles à l'obtention de ces données.

La circulaire rappelle également qu'en cas de risque de dissipation des données, un gel préalable des données peut être demandé lorsque les conventions internationales le permettent. Dès lors que les demandes sont justifiées par les nécessités de la procédure judiciaire, le chiffrement ou l'absence de réponse d'un fournisseur ne doivent pas dissuader les procureurs de formuler des demandes d'accès.

Pour les fournisseurs défaillants, leurs refus peuvent faire l'objet de remontées d'informations vers les parquets spécialisés, ainsi que de poursuites pénales.

Digital Omnibus on AI

Si l'Union européenne s'est dotée d'un véritable corpus juridique applicable à l'espace numérique, son application jugée complexe a amené la Commission européenne à publier, le 19 novembre 2025, deux propositions de règlements dites « Omnibus VII ».

La première, appelée Digital Omnibus, propose un ensemble de mesures transversales consacrées au numérique visant à alléger les réglementations liées à la cybersécurité et à la gestion des données personnelles. La seconde, appelée Digital Omnibus on AI, cible plus particulièrement le règlement européen sur l'intelligence artificielle.

Le 7 mai 2026, le Parlement européen et le Conseil de l'UE s'accordent sur le projet de règlement Digital Omnibus on AI. Il est entré en vigueur le 27 juillet 2026. L'autre texte demeure en discussion au sein du Conseil de l'Union européenne.

Les mesures prévues par ce texte prévoient notamment un report de l'entrée en application de certaines des obligations réglementaires prévues par le RIA.

Les exigences applicables aux systèmes d'IA à haut risque intégrés dans les produits (annexe I) entreront en application le 2 août 2028. Les obligations relatives aux systèmes d'IA à haut risque listés à l'annexe III entreront en application le 2 décembre 2027.

Est également prévue l'insertion de dispositions relatives à l'interdiction de systèmes d'IA qui génèrent ou manipulent soit des contenus représentant les parties intimes ou l'activité sexuelle d'une personne identifiable, sans son consentement, soit de la pédopornographie ou un « spectacle pédopornographique » au sens de la directive 2011/93/UE.

Règlement européen sur l'intelligence artificielle : projet de lignes directrices de la Commission sur la classification des systèmes d'intelligence artificielle à haut risque

Le 19 mai dernier, la Commission européenne a partagé son projet de lignes directrices sur la classification des systèmes d'intelligence artificielle à haut risque. Dépourvues d'effet juridique contraignant, elles visent à exposer l'interprétation, par la Commission, de certains concepts pertinents et contiennent des exemples pratiques de certains systèmes qui devraient, ou non, être classés à haut risque.

Le projet publié est subdivisé en sections et suit la structure de l'article 6 du règlement sur l'intelligence artificielle, qui identifie deux scénarios où un système d'intelligence artificielle serait considéré comme à haut risque :

- Le système est destiné à être utilisé comme composant de sécurité d'un produit, ou est lui-même un produit couvert par la législation d'harmonisation de l'UE énumérée à l'annexe I du règlement.
- Le système relève de l'un des cas d'utilisation énumérée dans les domaines de l'annexe III du règlement suivant lesquels il sera classé comme à haut risque.

Une consultation publique a été ouverte le 19 mai 2026 par la Commission européenne. Les parties prenantes avaient jusqu'au 23 juillet pour soumettre leurs observations. Les orientations finales devraient être adoptées d'ici la fin de l'année 2026.

Détection des abus sexuels sur mineurs en ligne : une dérogation temporaire à ePrivacy prévue par le règlement publié le 28 juillet 2026

Le règlement (UE) 2026/ 1881 du Parlement européen et du Conseil du 24 juillet 2026 prolonge la dérogation temporaire autorisant le traitement de données à caractère personnel, y compris relatives au contenu de communications, aux fins de détecter et de signaler des contenus déjà recensés comme relevant d'abus sexuels sur mineurs en ligne.

Il s'agit d'une dérogation à la confidentialité des communications garantie par les articles 5 et 6 de la directive ePrivacy du 12 juillet 2002, relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques.

Déjà prorogé une première fois jusqu'au 3 avril 2026, ce régime l'est de nouveau par le présent texte dans l'attente de l'adoption du règlement relatif à la lutte contre les abus sexuels sur les enfants, toujours en cours de négociations.

Réforme du démarchage téléphonique : mise en pratique depuis le 11 août 2026

Depuis le 11 août 2026, le démarchage téléphonique est interdit dans tous les secteurs, en application de la loi n° 2025-594 du 30 juin 2025 contre toutes les fraudes aux aides publiques.

Cette réforme adopte une logique d'opting in. Autrement dit, il appartient au consommateur de consentir expressément à la prospection commerciale par téléphone. L'article L. 223-1 du Code de la consommation prévoit deux cas suivants lesquels la prospection téléphonique sera possible. À savoir, lorsque le consommateur a donné au préalable son consentement clair à être prospecté ou, lorsque l'appel porte sur un contrat en cours.

Un régime de preuve numérique structuré et opposable est ainsi crée, renforçant la qualification pénale des pratiques de démarchage illicite et facilitant l'identification des données d'ordre dans les enquêtes cyber et pénales.

Sécurité intérieure – Publication de la loi « RIPOST », amputée de certaines de ses dispositions

La loi n° 2026-798 du 18 août 2026 visant à offrir des réponses immédiates aux phénomènes troublant l'ordre public, la sécurité et la tranquillité de nos concitoyens, dite loi RIPOST, a été promulguée le 18 août 2026. Elle a pour objectif la prévention et la répression de plusieurs infractions du quotidien et l'accroissement des moyens des forces de sécurité.

Elle donne des moyens d'action accrus aux forces de sécurité, à l'autorité administrative et à l'autorité judiciaire. Les possibilités d'emploi des dispositifs de lecture automatisée des plaques d'immatriculation (LAPI) sont étendues à de nouvelles infractions (vol aggravé, évasion, soustraction de mineur, aide à l'entrée ou au séjour irrégulier d'étrangers, etc.). Ces dispositifs pourront être également utilisés pour prévenir des actes de terrorisme ou certains troubles à l'ordre public.

La mise en œuvre, lors des Jeux Olympiques et Paralympiques de 2024, de l'expérimentation de la vidéosurveillance algorithmique est prolongée jusqu'au 31 décembre 2030. Sont concernés certains bâtiments ouverts au public et particulièrement exposés à des risques de terrorisme ou d'atteintes graves à la sécurité des personnes.

La loi entend également renforcer les moyens et la coordination des services participant à la lutte contre la criminalité organisée. À ce titre, elle durcit les règles d'exécution et d'aménagement de peines pour la criminalité organisée et prévoit le recours à des techniques spéciales d'enquête plus offensives pour des enquêtes complexes (trafic et usage de stupéfiants, usage détourné de protoxyde d'azote, rodéos urbains et rave-parties illégale et utilisation illicite et trafic de mortiers d'artifice). Les unités spécialisées dans la prévention et la répression des trafics de personnes et de biens bénéficieront de capacités de fouille et de contrôle d'identité aux frontières renforcées.

Règlement n° 2024/ 2847 dit Cyber Resilience Act visant à renforcer la cybersécurité des produits du numérique au sein de l'Union

Adopté le 23 octobre 2024, le Cyber Resilience Act (CRA) établit un cadre réglementaire applicable aux produits comportant des éléments numériques. À ce titre, il prévoit des règles relatives à la mise à disposition sur le marché de produits comportant des éléments numériques afin de garantir leur cybersécurité. Il pose notamment les exigences essentielles de cybersécurité relatives à la conception, au développement et à la production de produits comportant des éléments numériques et détermine les obligations applicables aux opérateurs économiques qui en découlent.

Ce règlement entrera progressivement en application entre juin 2026 et décembre 2027.

Depuis le 11 septembre 2025, le CRA oblige les fabricants à signaler sur la Plateforme Unique de Signalement, gérée par l'Agence de l'Union européenne pour la cybersécurité (ENISA), les vulnérabilités activement exploitées affectant les produits ayant des éléments numériques mis sur le marché intérieur de l'Union européenne ainsi que les incidents graves ayant un impact sur la sécurité du produit.

La notification est simultanément transmise au CERT-FR de l'ANSSI pour la France ou à l'ENISA, sauf circonstances exceptionnelles.

Commandement du ministère de l'Intérieur dans le cyberespace
#VEILLEJURIDIQUE n° 03 - SEPTEMBRE 2026

Directeur de la publication : GDI P. TOUAK
Responsable éditorial : LTN M. FISSEAU
Rédacteurs : LTN M. FISSEAU - Mme J. MERIOT
Conception graphique et maquettage : Mme M. BARREAU

En attendant le prochain numéro de la veille juridique, suivez notre actualité :

sur LinkedIn et sur X (ex-Twitter) : ***@ComCyberMI***