Crypto, TradFi & Digital

Spécial pixels de suivi : la question de la conformité e-mail

Décrypter la réglementation financière, IA et données pour anticiper, se conformer et décider

Pixels de suivi dans les e-mails : l'Europe resserre les règles

Les éditions précédentes du Regulatory Brief ont couvert les grands chantiers réglementaires européens : l'AI Act et son Omnibus (Éditions #7 et #18), son articulation avec le RGPD (Édition #8), la transition post-quantique (Édition #9), la souveraineté technologique (Édition #10), la convergence IA × cybersécurité (Édition #11), les abus de marché et la LCB-FT (Éditions #12, #14), la fin de la clause de grand-père MiCA (Édition #13), l'accélération réglementaire mondiale de l'IA (Édition #15), le vote du Parlement européen sur les stablecoins (Édition #16) et la protection des épargnants face aux arnaques crypto (Édition #17). Cette dix-neuvième édition ouvre une nouvelle dimension, celle des règles européennes de protection des données appliquées à une pratique aussi banale qu'invisible : les pixels de suivi dans les courriers électroniques.

Le 14 avril 2026, à l'issue d'une consultation publique menée en juin 2025, la CNIL a publié la version définitive de sa recommandation sur les pixels de suivi dans les courriels, adoptée par délibération n° 2026-042 du 12 mars 2026. Cette publication n'est pas isolée. Elle s'inscrit dans un mouvement européen convergent : le Garante italien a publié à peine trois jours plus tard, le 17 avril 2026, ses propres lignes directrices sur le sujet ; l'ICO (Information Commissioner's Office) britannique a suivi le 29 avril 2026 avec des lignes directrices définitives sur les pixels au titre du PECR (The Privacy and Electronic Communications (EC Directive) Regulations 2003). Le socle européen commun trouve son ancrage dans les lignes directrices 2/2023 du CEPD (Comité européen de la protection des données) adoptées dans leur version définitive le 7 octobre 2024, qui considèrent que l'insertion de pixels dans les e-mails constitue une opération de stockage et d'accès aux informations du terminal relevant de l'article 5(3) de la directive ePrivacy.

Pour tous les acteurs soumis au RGPD, notamment les acteurs financiers, l’enjeu est direct et opérationnel. Les newsletters commerciales, alertes clients, communications relatives aux comptes, campagnes de prospection et e-mails marketing s’appuient fréquemment sur des outils activant des fonctions de mesure des ouvertures et des clics. Les ouvertures sont généralement mesurées au

moyen d'un pixel invisible, tandis que les clics sont suivis au moyen de liens traçants ou de redirections individualisées. Ces deux techniques peuvent relever de l'article 5(3) de la directive ePrivacy, mais elles ne reposent pas sur le même mécanisme technique. La question posée par la CNIL et ses homologues est donc la suivante : dans quelles conditions l'observation du comportement du destinataire peut-elle être réalisée sans consentement et dans quelles conditions un consentement préalable est-il requis ?

Une échéance opérationnelle mérite d'être signalée dès l'ouverture. Pour les adresses collectées avant le 14 avril 2026, les organismes disposaient en principe de trois mois pour informer clairement les destinataires de l'utilisation de pixels et leur offrir un moyen simple de s'y opposer. Ce délai de principe a expiré le 14 juillet 2026. La FAQ publiée par la CNIL le 22 juillet précise toutefois qu'une prolongation raisonnable peut être admise lorsque des difficultés objectives liées au volume de la base ou à la délivrabilité sont justifiées et documentées. À défaut d'information dans le délai applicable, les pixels soumis au consentement doivent être désactivés ou faire l'objet d'un consentement valide. En Italie, le délai général de mise en conformité court jusqu'à la fin du mois d'octobre 2026.

Le signal faible

La conformité des communications électroniques ne se limite plus à la question : « Avons-nous le droit d'envoyer cet e-mail ? » Elle impose désormais une seconde question : « Avons-nous le droit d'observer ce que le destinataire en fait ? »

Cette évolution est plus structurante qu'il n'y paraît. Jusqu'à présent, la conformité opérationnelle de la prospection électronique s'est principalement concentrée sur la licéité de l'envoi : le consentement préalable au titre de l'article L. 34-5 du Code des postes et des communications électroniques pour les particuliers, le régime applicable à la prospection B2B et l'exception relative aux produits ou services analogues pour les clients existants. Les dispositifs de conformité ont ainsi été organisés autour de la distinction entre communications transactionnelles et communications promotionnelles. Cette distinction reste pertinente, mais elle ne suffit plus.

La seconde question porte sur l'opération technique de suivi. Le régime applicable aux pixels est juridiquement distinct de celui permettant l'envoi du courriel. Un e-mail transactionnel, une prospection B2B ou une communication adressée à un client existant peut être licitement envoyé sans consentement préalable à l'envoi, alors que le suivi individualisé qu'il contient demeure, en principe, soumis au consentement, sauf exemption applicable. Cette distinction appelle une revue des dispositifs d'e-mail marketing et de CRM ainsi qu'une configuration permettant l'envoi de messages dépourvus de suivi lorsque celui-ci n'est ni consenti ni exempté.

Focus 1 : La recommandation CNIL du 14 avril 2026

La recommandation de la CNIL, adoptée par la délibération n° 2026-042 du 12 mars 2026 et publiée au public le 14 avril 2026 après une consultation ouverte en juin 2025, s'adresse à tous les organismes, privés ou publics (entreprises, associations, administrations, collectivités) qui utilisent des pixels de suivi dans leurs courriels, ainsi qu'aux prestataires techniques auxquels ils peuvent avoir recours. Elle complète les lignes directrices 2/2023 du CEPD sur le champ d'application technique de la directive ePrivacy, et la recommandation « cookies et autres traceurs » de la CNIL.

Le régime juridique est clair : l'insertion d'un pixel constitue une opération de lecture ou d'écriture sur le terminal du destinataire relevant de l'article 82 de la loi Informatique et Libertés, qui transpose l'article 5(3) de la directive ePrivacy. Le consentement préalable, libre, spécifique, éclairé et univoque devient donc la règle lorsque le pixel est utilisé pour mesurer individuellement le taux d'ouverture d'une campagne, personnaliser le contenu ou la fréquence des messages, adapter le canal de communication, établir des profils d'intérêts, cibler ultérieurement la personne sur d'autres sites ou applications, ou détecter certaines fraudes en analysant individuellement les ouvertures. La CNIL précise qu'un consentement unique peut couvrir l'envoi d'une communication promotionnelle et l'utilisation de pixels ayant une finalité directement liée, par exemple lorsqu'une prospection est clairement présentée comme personnalisée. Les finalités sans lien direct doivent, en revanche, rester séparées.

Le consentement peut néanmoins ne pas être requis lorsque le pixel est exclusivement utilisé pour une finalité exemptée, notamment une mesure de sécurité participant à l'authentification ou une mesure de délivrabilité strictement nécessaire concernant un courriel demandé par l'utilisateur ou rattaché à un service qu'il a expressément demandé. Le caractère transactionnel du message ne suffit cependant pas, à lui seul, à justifier l'exemption : le courriel doit conserver un caractère exclusivement informatif ou fonctionnel, sans élément promotionnel, et toutes les autres conditions fixées par la recommandation doivent être respectées.

L'exemption peut également couvrir, dans des conditions strictes, l'identification des destinataires inactifs afin d'adapter la fréquence ou d'arrêter les envois, ainsi que la démonstration du respect de certaines obligations légales d'information. Pour la mesure individuelle de la délivrabilité, la CNIL recommande de ne conserver que la date de la dernière ouverture, sans l'heure, en remplaçant la donnée précédente à chaque nouvelle ouverture.

Ce qu'il faut surveiller

- Le cycle d'accompagnement de la CNIL : après un premier webinaire général organisé le 28 mai 2026, un webinaire destiné aux fournisseurs et prestataires a été organisé le 4 juin. La rediffusion de ce second webinaire et une FAQ détaillée ont été publiées le 22 juillet 2026.

- Les **premiers contrôles de la CNIL** sur les pratiques pixels : la CNIL a annoncé qu'elle veillerait au respect des règles dans le cadre de ses missions de contrôle à venir.
- L'articulation avec les **dispositifs cookies existants** et la nécessité d'aligner les pratiques CRM et emailing sur la recommandation cookies de la CNIL déjà en vigueur.

Focus 2 : Une convergence européenne coordonnée

La publication de la CNIL s'inscrit dans une convergence européenne marquée : trois autorités nationales ont publié, entre le 14 et le 29 avril 2026, des textes consacrés aux pixels ou aux technologies de stockage et d'accès. Ces positions reposent sur le socle commun des lignes directrices 2/2023 du Comité européen de la protection des données, adoptées dans leur version définitive le 7 octobre 2024. La convergence porte sur l'application des règles ePrivacy et sur la nécessité d'un consentement pour le suivi individualisé. Les exemptions et les modalités de mise en conformité demeurent toutefois différentes selon les juridictions.

Le Garante italien a publié le 17 avril 2026 des lignes directrices très proches de la position française. L'autorité italienne impose un consentement préalable pour la mesure individuelle des ouvertures, l'optimisation comportementale des campagnes et la création de profils commerciaux. Elle autorise en revanche, sans consentement, certains traitements : le calcul d'un taux global d'ouverture à condition que les résultats soient anonymes et qu'aucun pixel ne permette de distinguer les destinataires ; certaines mesures de sécurité et d'authentification ; les communications institutionnelles ou de service dont l'envoi est juridiquement obligatoire ; certaines alertes de sécurité, de fraude ou de phishing. L'utilisateur doit pouvoir retirer séparément son consentement au suivi tout en continuant, s'il le souhaite, à recevoir les e-mails. Le Garante recommande également l'utilisation d'identifiants non intelligibles et non séquentiels, conservés séparément des adresses électroniques. Les organismes disposent de six mois à compter de la publication des lignes directrices au Journal officiel italien le 29 avril 2026, soit jusqu'à la fin du mois d'octobre 2026, pour se mettre en conformité.

Au Royaume-Uni, l'ICO a publié le 29 avril 2026 des lignes directrices définitives précisant que les pixels intégrés aux e-mails relèvent des règles PECR relatives au stockage et à l'accès aux informations contenues dans un terminal, et non uniquement des règles applicables à l'envoi de communications commerciales. Les traitements strictement statistiques peuvent bénéficier d'une exemption lorsque les résultats sont agrégés, ne permettent pas d'identifier ou de suivre une personne et sont exclusivement utilisés pour améliorer le service, une information claire et un moyen d'opposition simple et gratuit restant nécessaires. Le suivi individuel, le profilage, le ciblage

publicitaire ou l'utilisation des données pour prendre des décisions concernant une personne continuent en revanche à nécessiter un consentement.

Une divergence importante doit être relevée. En France, le fait qu'un pixel collecte directement des données anonymes ou agrégées ne suffit pas à exempter cette collecte de consentement, l'article 82 de la loi Informatique et Libertés s'appliquant indépendamment du caractère personnel des données. En revanche, les données collectées licitement sur le fondement d'un consentement ou d'une exemption peuvent ensuite être anonymisées et réutilisées pour produire des statistiques globales. L'Italie et le Royaume-Uni reconnaissent, sous des conditions propres à leur droit national, des possibilités plus directes de recourir à des statistiques agrégées sans consentement.

Ce mouvement n'est pas isolé. Il s'inscrit dans une doctrine déjà exprimée par d'autres autorités : l'autorité danoise Datatilsynet avait, dès le 3 février 2023, adressé une critique sévère à un organisme ayant analysé les ouvertures et les clics de ses newsletters sans consentement valide ni information suffisante. Le BfDI allemand rappelle que le consentement à recevoir une newsletter ne couvre pas automatiquement l'utilisation de pixels : si le destinataire refuse le suivi, la newsletter doit pouvoir lui être adressée sans pixel. L'autorité irlandaise DPC considère également que les pixels, web beacons et technologies similaires nécessitent généralement un consentement dès lors qu'ils accèdent à des informations présentes sur le terminal.

Ce qu'il faut surveiller

- Les **prochaines lignes directrices ou communications d'autres autorités européennes** (BfDI, DPC, AEPD espagnole, autorités néerlandaise et belge), susceptibles de compléter la mosaïque et d'harmoniser les pratiques.
- La clarification des divergences relatives aux statistiques agrégées entre la CNIL, le Garante et l'ICO, notamment sur la distinction entre la collecte initiale au moyen du pixel et la réutilisation ultérieure de données anonymisées.
- Les **premières décisions de sanction** sur les pratiques pixels en 2026-2027, qui préciseront la portée effective des recommandations et les points de vigilance opérationnels.

Focus 3 - Ce qu'il faut vérifier : les points opérationnels

Les responsables du traitement, les DPO, directions marketing, DSI, directions juridiques, devraient désormais engager une revue systématique de leurs pratiques d'emailing et de CRM. Dix

points opérationnels ressortent de la lecture combinée des publications de la CNIL, du Garante et de l'ICO.

- Inventorier les **fonctions d'open tracking et de click tracking** activées dans les outils d'envoi et le CRM, en distinguant les pixels utilisés pour mesurer les ouvertures des liens traçants ou redirections utilisés pour mesurer les clics, ainsi que les statistiques agrégées du suivi individuel.
- Identifier **les données réellement collectées** via ces pixels (identifiant du destinataire, date, heure, appareil, adresse IP, géolocalisation approximative), leur précision et leurs destinataires (interne, prestataire, partenaire).
- Distinguer clairement les **statistiques agrégées du suivi individuel** : une frontière conceptuelle qui devient une frontière juridique.
- Documenter **séparément chaque finalité** (mesure d'audience, personnalisation, profilage, ciblage publicitaire, détection de fraude, mesure de délivrabilité, sécurité).
- Vérifier que les **exemptions invoquées sont réellement nécessaires et proportionnées** au regard des finalités poursuivies ; l'exemption doit être documentée et argumentée.
- Recueillir **le consentement au moment de la collecte de l'adresse** lorsque celui-ci est requis, avec les caractéristiques exigées par le RGPD et l'article 82 LIL (libre, spécifique, éclairé, univoque).
- Offrir un **mécanisme simple permettant de refuser ou de retirer uniquement le suivi**, sans compromettre la possibilité de continuer à recevoir la communication elle-même si celle-ci est licite.
- Revoir les **qualifications de responsable de traitement, sous-traitant ou responsable conjoint** avec les prestataires d'emailing ; un point souvent traité de façon expéditive dans les contrats standard.
- Conserver une **preuve individualisée du consentement** et des conditions dans lesquelles il a été recueilli, conformément à la doctrine constante de la CNIL en matière de charge de la preuve.
- Désactiver **par défaut les fonctionnalités de suivi** qui ne sont pas nécessaires ; le principe de minimisation devient un principe opérationnel de configuration des outils.

Focus 4 : Un chantier structurant pour les acteurs financiers

Le secteur financier occupe une place particulière dans ce nouveau paysage. Banques, assureurs, sociétés de gestion, courtiers, plateformes d'investissement, fintechs et prestataires de services sur crypto-actifs envoient de nombreux courriels à leurs clients et prospects : mouvements de compte, confirmations d'ordres, appels de marge, échéances contractuelles, alertes de sécurité, newsletters d'information financière, campagnes de prospection ou de fidélisation. Ces communications reposent souvent sur des outils d'e-mailing et des CRM qui proposent des fonctionnalités de suivi des ouvertures et des clics, parfois activées par défaut.

Trois cas d'usage doivent être analysés séparément.

Premièrement, les communications strictement transactionnelles ou réglementaires peuvent bénéficier d'une exemption lorsque le message est demandé par l'utilisateur ou se rattache directement à un service demandé, qu'il ne contient pas d'éléments promotionnels et que le pixel est limité à une finalité elle-même exemptée.

Deuxièmement, lorsqu'un utilisateur consent expressément à recevoir une newsletter personnalisée, un consentement unique peut couvrir l'envoi et les pixels directement nécessaires à cette personnalisation, sous réserve d'une information claire. En revanche, lorsqu'une communication est envoyée sans consentement sur le fondement de l'exception applicable aux produits ou services analogues, le pixel de délivrabilité ne bénéficie pas, de ce seul fait, d'une exemption et demeure en principe soumis au consentement.

Troisièmement, les communications de prospection B2B peuvent ne pas nécessiter de consentement à l'envoi, mais leur suivi individualisé reste, en principe, soumis au consentement, sauf exemption applicable dûment documentée.

Un point d'articulation important mérite d'être signalé pour les acteurs soumis au RGPD ainsi qu'à MiFID II, MiCA ou au Code monétaire et financier. Certaines communications imposées par une obligation légale ou réglementaire, telles que des informations précontractuelles, des modifications contractuelles ou certaines notifications obligatoires, peuvent bénéficier d'une exemption lorsque la mesure de l'ouverture est strictement nécessaire pour démontrer la transmission de l'information et que les autres conditions prévues par la CNIL sont réunies. Cette analyse doit être réalisée et documentée au cas par cas. Elle ne saurait couvrir automatiquement l'ensemble des communications d'un acteur régulé. Une revue technique et contractuelle des solutions d'e-mailing est donc prioritaire et pourra conduire, si nécessaire, à une adaptation ou une renégociation des contrats avec les prestataires.

Ce qu'il faut surveiller

- Les **communications AMF et ACPR** éventuelles sur l'articulation entre obligations d'information client sectorielles (MiFID II, MiCA, PRIIPs) et le régime des pixels, un sujet qui pourrait faire l'objet de clarifications sectorielles.

- Les **adaptations proposées par les principaux prestataires d'emailing** dans les mois qui viennent, notamment les configurations par défaut, les options de désactivation et la gestion différenciée du consentement.
- La **cohérence de la lecture supervisorielle française** AMF / ACPR / CNIL sur les communications réglementées, dans la logique d'articulation supervisorielle déjà décrite dans l'Édition #8.

À retenir

Cinq points structurants à intégrer :

- La recommandation de la CNIL s'inscrit dans une convergence européenne avec les positions du Garante italien et de l'ICO britannique, sur le socle des lignes directrices du CEPD. Les exemptions et modalités pratiques demeurent toutefois différentes selon les pays.
- Le consentement préalable s'impose par principe pour le suivi individualisé des ouvertures et des clics. Le régime du suivi est distinct de celui autorisant l'envoi du courriel, même si un même consentement peut parfois couvrir des finalités clairement liées.
- Les exemptions sont d'interprétation stricte et doivent être documentées au cas par cas. Le seul caractère transactionnel ou réglementaire d'un courriel ne suffit pas : le message doit notamment être demandé ou lié à un service demandé, et le suivi doit être strictement nécessaire à une finalité exemptée.
- En France, le délai de principe de trois mois a expiré le 14 juillet 2026. Une prolongation raisonnable peut toutefois être admise en présence de difficultés objectives, justifiées et documentées. En Italie, le délai général court jusqu'à la fin du mois d'octobre 2026.
- Les acteurs financiers doivent analyser séparément les communications transactionnelles ou réglementaires, les newsletters personnalisées consenties, les communications aux clients existants et la prospection B2B. Une revue technique et contractuelle des outils d'e-mailing est nécessaire.

Conclusion

La recommandation de la CNIL du 14 avril 2026 constitue davantage qu'une clarification technique. Elle formalise une seconde dimension de la conformité des courriels : après la question de la licéité de l'envoi vient celle de la licéité de l'observation du comportement du destinataire.

La convergence récente entre les autorités française, italienne et britannique, fondée sur la doctrine du CEPD et sur les positions antérieures d'autres autorités nationales, confirme que le suivi invisible des courriels devient un sujet autonome de conformité. Pour les acteurs financiers et les autres organisations envoyant d'importants volumes de courriels, l'enjeu est immédiat : il appelle une revue systématique des pratiques, une adaptation technique et contractuelle des outils d'e-mailing et une collaboration étroite entre les directions juridiques, les DPO et les équipes marketing.

Sources principales

- CNIL, *« Pixels de suivi dans les courriers électroniques : la CNIL publie ses recommandations pour mieux protéger la vie privée »*, publication du 14 avril 2026 ; *Délibération n° 2026-042 du 12 mars 2026 portant adoption d'une recommandation relative aux pixels de suivi dans les courriers électroniques* (JORF, ref. JORFTEXT000053876850) ; recommandation téléchargeable sur cnil.fr.
- CNIL, *Synthèse des contributions à la consultation publique* et *Synthèse des contributions à la consultation sur les enjeux économiques*, publiées le 14 avril 2026 (cnil.fr).
- CNIL, *Webinaire du 22 juillet 2026 sur les pixels de suivi (fournisseurs et prestataires)* et *FAQ – Questions-réponses relatives à la recommandation pixels de suivi*, publiée le 22 juillet 2026.
- CEPD (Comité européen de la protection des données), *Lignes directrices 2/2023 sur le champ d'application technique de l'article 5(3) de la directive ePrivacy*, version définitive adoptée le 7 octobre 2024 (edpb.europa.eu).
- Garante italien (Garante per la Protezione dei Dati Personali), *lignes directrices sur les pixels de suivi dans les courriers électroniques*, publiées le 17 avril 2026, entrées en vigueur avec la publication au Journal officiel italien du 29 avril 2026.
- ICO (Information Commissioner's Office, Royaume-Uni), *Guidance on tracking pixels under PECR*, version définitive publiée le 29 avril 2026 (ico.org.uk).
- Datatilsynet (Danemark), *décision du 3 février 2023* relative à l'utilisation de pixels dans les newsletters sans consentement valide.
- BfDI (Allemagne), *recommandations sur les newsletters et pixels de suivi* ; DPC (Irlande), *guide sur les cookies et technologies de suivi*.
- Directive 2002/58/CE (ePrivacy), article 5(3) ; loi n° 78-17 du 6 janvier 1978 (Informatique et Libertés), article 82.
- Règlement (UE) 2016/679 (RGPD) ; cadre général des traitements de données personnelles.

***

The Seqlense Regulatory Brief - Crypto & TradFi · Édition #19

Cette publication est fournie à titre strictement informatif et ne constitue ni un conseil en investissement, ni une recommandation personnalisée, ni une incitation à acheter ou vendre des instruments financiers ou des crypto-actifs.

Les informations présentées reflètent une analyse générale des dynamiques de marché et des évolutions réglementaires à la date de publication. Elles ne tiennent pas compte de la situation personnelle, des objectifs d'investissement ni du profil de risque de chaque lecteur.

Malgré les soins apportés à la sélection et à la vérification des sources, aucune garantie n'est donnée quant à l'exactitude, l'exhaustivité ou l'actualité des informations. Les marchés financiers et les crypto-actifs présentent des risques élevés, notamment de volatilité et de perte en capital.

En conséquence, toute décision d'investissement relève de la seule responsabilité du lecteur et doit, le cas échéant, être prise avec l'appui de conseillers professionnels qualifiés.