Consultation publique sur le projet de recommandation relative aux pixels de suivi dans les courriers électroniques

Synthèse des contributions de la consultation publique et réponses de la CNIL

Avril 2026

Le 12 juin 2025, la CNIL a lancé une consultation publique sur son projet de recommandation relative aux pixels de suivi dans les courriers électroniques afin de recueillir les difficultés d'interprétation suscitées par le texte. Les contributions ont alimenté les travaux de la CNIL en vue de la publication de la version définitive de la recommandation.

Cette synthèse présente les observations les plus importantes ainsi que les éléments de réponse que la CNIL a décidé de leur apporter.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La synthèse en chiffres

Le projet de recommandation a reçu les contributions de 69 **personnes lors de la consultation publique** :

- 33 contributions provenant du secteur privé (entreprise, associations professionnelles).
- 26 contributions provenant de particuliers.
- 5 contributions d'associations de la société civile.
- 3 contributions d'autorités de protection des données en Europe.
- 1 contribution d'un organisme du secteur public.
- 1 contribution provenant du monde académique.

Ces contributions ont permis à la CNIL :

- de vérifier le caractère opérationnel du projet de recommandation au regard des contraintes, notamment techniques, auxquelles les acteurs sont soumis ;
- de le faire évoluer afin de prendre en compte les préoccupations les plus fréquemment partagées par les contributeurs.

Observations générales

Synthèse des contributions

Certains contributeurs se sont demandé si d'autres recommandations seront publiées sur d'autres technologies similaires, comme les liens traçants ou les mesures de prise d'empreinte numérique unique (*fingerprinting*).

Éléments de réponse de la CNIL

Ces technologies sont également couvertes par l'article 82 de la loi Informatique et Libertés (voir les lignes directrices 2/2023 du CEPD sur le champ d'application technique de l'article 5, paragraphe 3, de la directive vie privée et communications électronique (ci-après, la directive « ePrivacy »))[1].

Le critère clé pour déterminer si le consentement est requis repose davantage sur les finalités que sur la technologie elle-même. Que l'on parle de témoins de connexion (cookies), de pixels, d'empreintes numériques uniques (*fingerprinting*) ou d'autres traceurs, c'est l'usage qui en est fait qui détermine s'il faut recueillir le consentement ou si une exemption est applicable.

Dès lors, la recommandation « cookies et autres traceurs » et celle sur les pixels dans les courriels devraient permettre aux acteurs de guider leur analyse sur d'autres technologies, conformément au principe de responsabilité.

[1] Lignes directrices 2/2023 du CEPD sur le champ d'application technique de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques. Disponible ici : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_fr.

Sur l'application 82 de la loi Informatique et Libertés aux pixels

Synthèse des contributions

Des contributeurs ont contesté ou interrogé l'application de l'article 82 de la loi Informatique et Libertés aux pixels de suivi. Ils ont considéré que la CNIL :

- élargissait le concept d'« *accès à des informations stockées dans le terminal* » en l'appliquant à des technologies où le serveur collecte passivement des données techniques automatiquement transmises par le terminal via une requête HTTP. Ils ont rappelé que ce processus correspond en réalité à un comportement standard du protocole web, ce qui est notamment le cas des pixels de suivi.
- ne tenait pas compte de l'impact réel de ces technologies pour les utilisateurs en rejetant une approché fondée sur les risques.

Éléments de réponse de la CNIL

Les lignes directrices 2/2023 du CEPD, transposé en droit français à l'article 82 de la loi Informatique et Libertés, rappellent l'application de ces dispositions aux pixels insérés dans les courriels.

La recommandation a également été complétée sur ce point (section « 2.1 Technologies et environnements concernés » de la partie 2.1 de la recommandation).

Sur l'exemption au consentement pour certains pixels dans les courriels électroniques (partie 3.2 de la recommandation)

Synthèse des contributions

Certains contributeurs ont sollicité une application stricte de la règlementation et une absence totale d'exemption. À l'inverse, d'autres contributeurs ont argumenté en faveur d'une ouverture des exemptions.

L'exemption relative à la mise en œuvre des mesures de sécurité de l'authentification de l'utilisateur

Pour certains contributeurs, cette exemption ne se justifiait pas car l'apport en termes de sécurité n'est pas clairement identifié. En particulier, des méthodes alternatives seraient possibles (utilisant des cookies) et cette mesure de sécurité serait, dans les faits, d'un intérêt très limité car le blocage des pixels est possible.

D'autres, à l'inverse, se sont interrogés sur la possibilité d'élargir l'exemption liée à la sécurité à la finalité de détection et lutte contre la fraude. Certains contributeurs ont avancé que l'identification d'ouvertures de courriels inhabituelles ou massives, susceptibles d'indiquer un comportement automatisé, devrait pouvoir bénéficier de l'exemption de consentement et reposer sur l'intérêt légitime car ce traitement a pour seul objectif de sécuriser la communication électronique contre des comportements nocifs similaires à des attaques par déni de service distribué (*Distributed Denial of Service* ou DDOS, en anglais). Les finalités de protection des infrastructures techniques et de protection des personnes viseraient un même objectif fondamental : protéger les utilisateurs et les systèmes contre les comportements malveillants.

Certains contributeurs ont identifié une incohérence entre la doctrine de la CNIL dans le contexte du web (qui admet une exemption pour lutter contre le DDOS) et celle des courriels (qui n'admet pas l'usage de traceurs pour la détection d'ouvertures automatisées potentiellement massives).

L'exemption relative à la mesure de la délivrabilité des courriels

De nombreux contributeurs ont considéré, au contraire, que la portée de l'exemption n'est pas suffisante car le taux global permet uniquement de constater une difficulté de délivrabilité, sans pouvoir la corriger en retirant les « inactifs » :

- La limitation de l'exemption à la mesure globale du taux d'ouverture ne permet pas aux acteurs d'agir efficacement sur la délivrabilité des messages. L'absence de mesure individuelle – du fait de l'absence de pixel ou de consentement à son activation – fait peser le risque pour l'entité en charge de l'envoi des courriels d'être placée sur une « liste noire » ou de voir les messages requalifiés en *spam* dès les premiers envois. En effet, le taux des courriels lus est l'un des critères utilisés afin de détecter et bloquer les spammeurs ; cet indicateur conduit à associer un score à un envoyeur (ou à son domaine d'envoi) et conditionne sa capacité à faire parvenir ses courriels à leurs destinataires. Les pixels permettraient de préserver ce score en supprimant des listes de diffusion les utilisateurs identifiés comme inactifs (ceux qui n'ouvrent pas leurs courriels).
- L'absence de mesure individuelle de l'ouverture pourrait conduire à des envois moins pertinents pour les destinataires et, donc, à un accroissement du volume de courriels indésirés.

Ces contributeurs ont souligné l'intérêt de l'usage de pixels à la fois pour eux (limiter l'envoi aux personnes intéressées) mais aussi pour les utilisateurs (prendre en compte leur souhait de ne plus recevoir de courriel du fait de l'absence d'ouverture de ces derniers, palliant l'usage trop peu fréquent du lien de désinscription).

Ainsi, de nombreux contributeurs professionnels ont considéré que cette mesure individuelle devait permettre :

- de mesurer la performance des listes de diffusion ;
- d'apporter la preuve de la réception du courriel pour démontrer le respect d'une obligation légale, notamment s'agissant des courriels transactionnels et de notification de violation de données ;
- d'évaluer et adapter le canal de communication notamment pour les courriels transactionnels et de notification de violation de données afin de contacter le destinataire par le biais d'un canal alternatif/différent pour assurer sa bonne information.

Enfin, certains contributeurs ont indiqué communiquer les données d'horodatage auprès des organismes contrôlant le respect de leurs obligations légales ou réglementaires et mettent en avant la **nécessité de pouvoir disposer d'un horodatage complet** (date et heure de réception des courriels de chaque destinataire).

Éléments de réponse de la CNIL

L'exemption relative à la mise en œuvre des mesures de sécurité de l'authentification de l'utilisateur

La lutte contre la fraude est un objectif souvent légitime dans le contexte de la fourniture d'un service en ligne.

Toutefois, comme la CNIL l'a rappelé dans le cadre de ces travaux sur les « cookies et autres traceurs » sur le web (voir la question / réponse n° 16 de la FAQ « cookies et autres traceurs »)[2] :

- Les traceurs utilisés à des fins de lutte contre la fraude, de manière générale, n'entrent pas dans les exemptions prévues par l'article 82 de la loi Informatique et Libertés.
- Toutefois, si ces traceurs visent à assurer la sécurité d'un mécanisme d'authentification de l'utilisateur (par exemple, en limitant les tentatives d'accès robotisées ou inattendues) ou à assurer la disponibilité du service demandé par l'utilisateur (par exemple en protégeant contre des attaques en menaçant la disponibilité technique de type DDoS), ils peuvent être regardés comme nécessaires au service demandé par l'utilisateur (sécurité centrée sur l'utilisateur).

S'agissant des courriels, l'analyse finalement retenue par la CNIL s'inscrit dans une logique identique :

- La lutte contre la fraude ne constitue pas, en tant que telle, une finalité justifiant une exemption.

[2] Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la CNIL. Disponible ici : https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ.

- L'utilisation de pixels ayant pour objet de contribuer à la sécurisation de l'authentification des utilisateurs est considérée comme exemptée. En revanche, le contexte technique lié à l'envoi de courriels ne se prêtant pas, en pratique, à des attaques en déni de service[3] visant les expéditeurs, il n'apparaît pas nécessaire de préciser l'applicabilité d'une exemption à de telles hypothèses.

L'exemption relative à la mesure de la délivrabilité des courriels

La recommandation reconnaît et encadre l'existence d'une exemption au consentement pour la mesure individuelle de la délivrabilité des courriels rattachés à un service demandé par le destinataire (voir le point 3.2 de la recommandation).

Synthèse des contributions

Plusieurs contributeurs ont considéré que le pixel de suivi ne peut jamais être un service demandé par l'utilisateur ou n'ont pas identifié pas de courriels pouvant particulièrement se rattacher à une telle notion.

D'autres contributeurs se sont fermement opposés à la position du projet de recommandation considérant que le pixel, qui est purement fonctionnel et intrinsèquement lié à l'envoi du message, devait suivre le même régime juridique que le message lui-même.

Toutefois, en réponse à la question posée par la CNIL dans son questionnaire, certains contributeurs ont considéré qu'un pixel de suivi s'attache à un service demandé par l'utilisateur lorsqu'il est utilisé dans les cas suivants :

- Communications expressément sollicitées par les utilisateurs ou nécessaires aux services demandés dont notamment les courriels dits « transactionnels ».
- Courriels mercatiques (*marketing*) adressés en l'absence d'opposition (produits ou services analogues, prospection à l'attention des professionnels, prospection caritative etc.).
- Lettres d'informations ou alertes éditoriales (alertes météo, offres d'emploi, enquête clients après l'achat d'un produit / la délivrance d'un service) ou commerciales (bons plans, actualités sectorielles).
- Courriels diffusés à la suite d'une violation de données personnelles susceptible d'entrainer un niveau de risque élevé (article 34 du RGPD).

Certains contributeurs ont également visé tous les courriels pour lesquels un consentement a été donné (comme les lettres d'informations ou communications promotionnelles auxquels la personne s'est abonnée).

D'autres contributeurs ont proposé d'exempter, sous certaines conditions (information des personnes, absence d'utilisation à d'autres fins, collecte de la seule information sur l'ouverture sans la localisation, l'horodatage, limitation de l'accès aux données, suppression à la fin de la campagne), l'utilisation de pixels de suivi à des fins de mesure individuelle de l'ouverture des courriels lorsque ceux-ci sont embarqués dans les courriels que diffuse un responsable de traitement aux personnes concernées :

- pour délivrer des informations critiques pour la santé et la sécurité des personnes concernées (rappels de produits défectueux, alertes sanitaires, etc.) ou ayant une importance particulière en termes de droits (notifications de changements de conditions contractuelles, informations sur des droits légaux importants).
- pour délivrer les notifications de service public (incidents majeurs dans les services de transport, alertes de sécurité publique, catastrophes naturelles, etc.).
- pour permettre aux professionnels de santé de se connecter facilement à une plateforme/site web d'un laboratoire pour obtenir des informations auxquelles seuls les professionnels de santé peuvent accéder.

Éléments de réponse de la CNIL

Dans la mesure où l'article 82 de la loi Informatique et Libertés évoque une « demande expresse » de l'utilisateur, ces exemptions ne peuvent concerner que les courriels demandés par le destinataire ou qui se rattachent à un service demandé par ce dernier.

La recommandation apporte donc des précisions sur les courriels qui peuvent être rattachés à un service demandé par le destinataire (voir la partie 3.2 de la recommandation). Elle permet également aux courriels de l'administration adressés dans le cadre de leur mission de service public, en particulier ceux envoyés dans le

[3] Le site cybermalveillance.gouv.fr définit l'attaque par déni de service comme une attaque « *visant à rendre inaccessible un serveur grâce à l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation de faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service*. ».

cadre de démarches proactives bénéficiant à l'usager (information sur la possibilité de bénéficier d'un droit), de bénéficier des exemptions rappelées dans la recommandation.

Sur les modalités pratiques du recueil du consentement (partie 4.2 de la recommandation)

Synthèse des contributions

Certains contributeurs ont favorablement accueilli l'approche de la CNIL sur la possibilité de recueillir un consentement unique pour un courriel le nécessitant (par exemple, la prospection par voie électronique) et pour l'usage de pixels de suivi pour des finalités connexes.

Toutefois, des clarifications sont demandées sur la possibilité de recueillir un consentement unique pour l'ensemble des finalités (courriels et toutes les finalités justifiant l'usage de pixels) listées dans le projet de recommandation sans nécessité de permettre un consentement granulaire.

Éléments de réponse de la CNIL

La recommandation précise que, pour assurer le caractère libre du consentement et dans l'hypothèse où les pixels poursuivent eux-mêmes plusieurs finalités distinctes, le consentement doit être obtenu de façon indépendante et spécifique lorsque ces finalités ne sont pas connexes (voir la section « L'expression d'un consentement libre » de la partie 4.2 de la recommandation).

Synthèse des contributions

Plusieurs contributeurs ont également fait valoir que :

- Les modalités de recueil du consentement identifiées par la CNIL (formulaire lors de la collecte de l'adresse électronique concernée ou envoi d'un premier message) seraient techniquement complexes et impraticables en termes d'expérience utilisateur.
- Un contributeur a sollicité d'autres modalités pour les organismes publics qui envoient des courriels dont la base légale de cet envoi est soit l'obligation légale soit la mission d'intérêt public.
- Certains professionnels ont regretté que le projet de recommandation soumis à consultation n'ait pas évoqué la possibilité d'un recueil du consentement pour les pixels via une plateforme de gestion du consentement (*consent management platform* ou CMP) affichée à l'arrivée sur un site web/une application mobile également. Ils considèrent que les plateformes de recueil du consentement doivent être privilégiées pour tous les traceurs.

Éléments de réponse de la CNIL

Les recommandations de la CNIL ont notamment vocation à accompagner les professionnels dans le respect du caractère éclairé du consentement. En effet, le destinataire doit être conscient de la portée du consentement qu'il envisage de donner ce qui implique notamment de lui permettre d'identifier l'adresse électronique qui sera concernée par l'utilisation des pixels de suivi.

La recommandation contient désormais un point d'attention sur le recueil du consentement via une CMP (voir l'encadré « Le recueil d'un consentement aux pixels via une plateforme de gestion du consentement (consent management platform ou CMP) » dans la section « L'expression d'un consentement libre » de la partie 4.2 de la recommandation).

Sur le retrait effectif du consentement s'agissant des pixels de suivi intégrés dans des courriels déjà envoyés (partie 5 de la recommandation)

Synthèse des contributions

Plusieurs contributeurs ont signalé l'absence, à ce jour, de solution technique simple et fiable pour empêcher de nouvelles opérations de lecture lorsque le destinataire ouvre à nouveau son courriel après avoir retiré son consentement aux pixels. Cela justifie, pour certains une interdiction stricte de cette pratique alors que, pour d'autres, cela signifie uniquement que le retrait du consentement doit être orienté pour l'avenir et non le passé.

Certains contributeurs ont proposé des méthodes pour prendre en compte le retrait du consentement :

- Certains contributeurs ont souligné que la seule méthode garantissant la non-réactivation du pixel dans un ancien message **est la désactivation du nom de domaine utilisé dans l'adresse** (URL) du pixel.
- Pour d'autres, il pourrait être acceptable de mettre en place des mesures techniques pour rejeter les requêtes et donc bloquer leur analyse.
- Enfin certains contributeurs ont évoqué la possibilité « d'anonymiser » les requêtes en continuant de les accepter mais en bloquant l'association à l'utilisateur individuel.

Éléments de réponse de la CNIL

Le responsable du traitement doit s'assurer de l'effectivité du retrait du consentement : en principe, les opérations de lecture ou d'écriture concernées par ce retrait ne peuvent plus avoir lieu lors de l'envoi de courriels à venir.

S'agissant toutefois des courriels déjà envoyés, étant donné le contexte technique spécifique et en l'absence de solutions techniques convaincantes pour bloquer la réception même de ce pixel, la recommandation impose de mettre en œuvre des mesures pour assurer l'absence d'exploitation du pixel.

Sur l'application de la recommandation aux bases de données déjà constituées (partie 7 de la recommandation)

Synthèse des contributions

De nombreux contributeurs ont critiqué l'application de la recommandation aux bases de données déjà constituées et appelé à **la création d'une exemption pour les bases de données préexistantes** :

- ils ont souligné le « caractère récent de l'interprétation doctrinale qualifiant les opérations techniques liées aux pixels de mails comme relevant de l'article 82 de la loi Informatique et Libertés » craignant d'éventuelles sanctions au titre des envois de courriels contenant des pixels antérieurs à la recommandation ;
- ils ont proposé notamment qu'une simple information permette cette régularisation.

Par ailleurs, certains contributeurs ont considéré que, compte tenu des changements profonds qu'impliquerait une telle recommandation, un long délai de mise en conformité devrait être octroyé aux professionnels (six mois à une année).

Éléments de réponse de la CNIL

La CNIL a décidé d'adopter une approche progressive : pour les courriels envoyés à des adresses collectées **avant** la publication de la recommandation, il est seulement demandé aux acteurs, dans un délai de **trois mois**, d'**informer clairement** les destinataires de l'utilisation de pixels pour **les mettre en mesure de s'y opposer facilement** s'ils le souhaitent.