

Pixels de suivi

Consultation publique

Association PURR

20 juillet 2025

Par ce présent mémoire, notre association entend participer à la consultation organisée par la CNIL en ce qui concerne le projet de recommandation sur les pixels traçants.

Vous trouverez donc ci-après notre position.

TABLE DES MATIÈRES

1	Sur le contexte de cette consultation	4
2	Sur la licéité des pixels traçants	5
2.1	Sur l'obligation de consentement	5
2.2	Sur la proportionnalité des pixels traçants	7
2.3	Sur les moyens alternatifs	7
2.4	Sur la demande exclusive de la Personne Concernée	8
2.5	Sur l'attente raisonnable d'une Personne Concernée	8
2.6	Sur la fragmentation de l'application du RGPD en Europe	8
3	Sur le contenu de la recommandation	10
3.1	Sur la pertinence des questions posées	10
3.2	Sur le périmètre technologique (§2.1)	10
3.3	Sur les acteurs concernés (§2.2)	11
3.4	Sur la différence entre la directive ePrivacy et sa transposition en droit national (§3)	11
3.5	Sur les finalités exemptées de consentement (§3.2)	12
3.5.1	Sur les mesures de sécurité	12
3.5.2	Sur les mesures du taux d'ouverture global	13
3.5.3	Sur le périmètre des courriels	14
3.5.4	Sur la nécessité pour la délivrabilité	14
3.5.5	Sur la multiplicité des bases légales	15
3.6	Sur la réutilisation des données et l'anonymisation	16
3.7	Sur les modalités de recueil du consentement (§4.2)	16
3.7.1	Sur les modalités d'information	16
3.7.2	Sur la durée de rétention du refus de consentir	16
3.7.3	Sur l'expression libre du consentement	17
3.7.4	Sur la connexité	17
3.7.5	Sur l'encart d'exemption au titre de l'article 82 de la LIL	18
3.8	Sur le retrait et la gestion du consentement (§5)	18

3.9	Sur l'opposition	20
3.9.1	Sur l'automatisation de l'opposition	20
3.9.2	Sur les moyens techniques d'opposition	20
3.10	Sur le défaut d'instruction de la CNIL	21
4	Conclusion	23

1 SUR LE CONTEXTE DE CETTE CONSULTATION

À titre liminaire, notre association souhaite rappeler la problématique déjà soulevée devant le Conseil d'État¹ de l'organisation partielle de concertations privées préalablement à cette consultation publique.

Nous rappelons que, dès 2022, la CNIL disposait d'une doctrine imposant le consentement aux pixels de suivi².

Nous savons que, dès septembre 2023, préalablement à cette consultation, la CNIL a organisé, avec les Responsables de Traitement, des réunions, plusieurs ateliers, une cartographie des usages³, etc.

Nous nous retrouvons donc aujourd'hui à participer à une unique consultation biaisée et à laquelle il a été refusé à notre association de participer aux phases préliminaires.

D'un côté, les Responsables de Traitement ont pu longuement exposer leurs besoins, échanger avec la CNIL, obtenir des précisions et explications sur le contenu du projet de recommandation, etc.

De l'autre côté, les Personne Concernée et les DPO doivent se contenter, pendant un seul mois et en pleine période estivale, d'un formulaire web de quatre questions pour répondre à un projet de recommandation déjà prêt que les Responsables de Traitement ont pu faire amender en amont selon leurs besoins.

Il en ressort une inégalité manifeste dans l'accès à la CNIL et dans le poids de l'expression de chaque catégorie de partie-prenante : les Responsables de Traitement ont été très clairement favorisés une fois encore.

En outre, il sera rappelé que, depuis un an et demi, la CNIL a opposé la seule existence de ces concertations privées pour clôturer en masse des réclamations sans les instruire et sans adopter de mesures correctrices⁴, faisant fi de la constitution des faits pour le passé⁵.

Cette concertation n'est une fois encore qu'un prétexte pour votre Commission afin ne pas sanctionner ces manquements par une légalisation de pratiques pourtant illicites.

1. Recours en annulation de la concertation préalable à cette consultation publique, affaire n° 500982

2. <https://web.archive.org/web/20220202161825/https://www.cnil.fr/fr/nouvelles-methodes-de-tracage-en-ligne-quelles-solutions-pour-se-proteger>; https://www.cnil.fr/sites/cnil/files/2023-05/cnil_-_43e_rapport_annuel_-_2022.pdf, page 78; et <https://www.cnil.fr/fr/revoir-le-webinaire-evolution-des-regles-applicables-en-matiere-de-cookies-et-autres-traceurs-bilan>, 24 minutes 20.

3. <https://alliancecommerce.org/pixels-de-suivi-presentation-et-concertation-de-la-cnil/>

4. Exemples : réclamations n°s 44-42208, 44-962, 44-1094, 44-1107, 44-1492, 44-1747, 44-1831, 44-26034, 44-26175, 44-26284, 44-39687

5. En ce sens, délibération SAN-2024-002 de la CNIL

Il sera rappelé que les manquements sont graves puisqu'il s'agit de correspondance privée et de consentement, principes fondamentaux du RGPD, certainement même les plus importants de cette législation.

La chronologie de l'organisation de cette consultation, après celle des lignes directrices cookies et celle sur le consentement cross-device, est une nouvelle fois très claire : des Responsables de Traitement dans la plus totale illécéité sont venus voir votre Commission pour s'arranger pour ne jamais être sanctionnés pour les manquements antérieurs à la publication de cette recommandation et pour ne plus rien craindre une fois celle-ci publiée, malgré que leurs traitements n'en restent pas moins toujours totalement illicites.

2 SUR LA LICÉITÉ DES PIXELS TRAÇANTS

2.1 Sur l'obligation de consentement

Dans son introduction, votre Commission fait plusieurs références aux lignes directrices du CEPD, dont celles 02/2023 portant, entre autres, sur l'assujettissement des pixels de suivi à la directive ePrivacy.

Il semble étonnant que votre Commission omette ici le document de référence en matière de pixels de suivi dans les courriels, à savoir l'avis WP118 du WP29 du 21 février 2006⁶.

En effet, cet avis contient une section explicite applicable aux pixels traçants :

Le groupe 29 observe le développement d'un nouveau type de logiciels et de services, comme le «DidTheyReadIt» («l'ont-ils lu?») qui permet de vérifier si un message a été ouvert.

Ce service met toute personne qui y est abonnée en mesure de savoir a) si les destinataires de ses messages électroniques les ont lus, b) à quel moment, c) combien de fois ils les ont lus (ou, au moins, ouverts), d) s'ils les ont transmis à d'autres personnes, et e) vers quel serveur de messagerie, y compris sa localisation. Enfin, il permet également de connaître le navigateur utilisé par le destinataire ainsi que son système d'exploitation.

6. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp118_fr.pdf

Le traitement des données se déroule à l'insu des destinataires des messages électroniques, c'est-à-dire qu'ils ne reçoivent aucune information sur le traitement de données dont ils font l'objet. De plus, ils n'ont pas le choix d'accepter ou de refuser cette extraction d'informations. En résumé, à la différence des services «classiques» d'accusé de réception de messages, le destinataire n'a pas la possibilité d'accepter ou de refuser de retourner les informations à l'utilisateur du logiciel.

Le groupe 29 émet les plus vives réserves sur ce procédé car des données personnelles sur le «comportement» du destinataire sont ainsi enregistrées et transmises sans qu'il y ait eu consentement indubitable de sa part. **Un tel traitement, effectué à l'insu des personnes concernées, est contraire aux règles de protection des données qui exigent loyauté et transparence dans la collecte des données à caractère personnel, conformément à l'article 10 de la directive sur la protection des données.**

Pour pouvoir réaliser le traitement de données consistant à rechercher sur le terminal du destinataire d'un courriel s'il l'a lu, quand il l'a lu et s'il l'a transmis à des tiers, **son consentement indubitable est nécessaire. Aucun autre argument juridique ne saurait justifier ce traitement.** Par conséquent, un traitement de données effectué à l'insu des personnes concernées est contraire aux règles de protection des données qui exigent un consentement donné indubitablement, ainsi qu'en dispose l'article 7 de la directive sur la protection des données.

Le WP29, dorénavant le CEPD, est ici très clair sur la seule et unique possibilité légale d'existence d'un traitement en lien avec des pixels traçants dans les courriels : le strict consentement.

Toute autre base légale, et en particulier l'intérêt légitime, semble en effet disproportionnée au regard de l'intrusion dans la vie privée des Personnes Concernées par rapport à la frivolité des finalités visées en pratique.

Il sera rappelé que l'avis 02/2006 est référencé dans WP187⁷, elles-mêmes ensuite pointées par le CEPD dans ses lignes directrices 05/2020⁸. De même, l'EDPS pointe vers WP118 dans son avis 6/2017⁹.

Les pixels traçants ne remplissant pas et ne pouvant respecter les critères de loyauté et de transparence prévus à l'article 5 du RGPD, ils en sont illicites.

7. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, section III.B.2

8. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_fr

9. https://www.edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf, annexe 9

2.2 Sur la proportionnalité des pixels traçants

Nous rappelons vivement que la correspondance privée, fut-elle transactionnelle, n'est pas assimilable ni comparable à un service d'édition public comme un site web.

L'intrusion dans la correspondance privée est perçue, à juste titre, par les personnes, comme une intrusion forte dans leur intimité, comme la CNIL l'a relevé dans sa délibération SAN-2024-019 contre Orange SA.

Le CEPD et la CJUE sont très clairs : les intérêts du Responsable de Traitement doivent être factuels, avérés et non spéculatifs¹⁰. Les finalités visées par les Responsables de Traitement sont au contraire très frivoles, supputatives voire inexistantes comme nous le verrons par la suite et leur intérêt n'est en tout état de cause pas démontré.

L'ajout de pixels traçants dans de la correspondance privée reste donc une ingérence grave dans les droits des Personnes Concernées et constitue un traitement manifestement disproportionné au regard des finalités visées.

Les pixels traçants ne répondent donc pas aux obligations prévus aux articles 5 et 6 du RGPD.

Une nouvelle fois, ce type de traitement est donc illicite.

2.3 Sur les moyens alternatifs

Le CEPD¹¹ ainsi que la CJUE¹² sont aussi parfaitement clairs qu'un traitement est *de facto* illicite s'il existe un moyen moins intrusif de parvenir à la même finalité.

Or nous rappelons qu'il existe des techniques de suivi normalisées réalisant la finalité visée par les Responsables de Traitement :

- Delivery Status Notifications, RFC 1894 et 3464 : notifications sur l'état de la livraison d'un courriel
- Message Disposition Notification, RFC 2298, 3798 et 8098 : accusés de lecture d'un courriel

Elles n'ont cependant jamais connu un très grand essor justement parce que les Personnes Concernées étaient généralement très peu enclines à accepter ce type de suivi, même quand leur consentement était ici parfaitement respecté.

Cela donne ainsi un indice sur leur rejet de ce type de mesure par les Personnes Concernées.

En pratique, comme présenté auparavant, la recommandation de la CNIL vise exclusivement à contourner en réalité ce rejet massif par des traitements difficiles sinon impossibles à contourner par une Personne Concernée, à supposer même qu'elle en soit ne serait-ce qu'informée.

10. Lignes directrices 01/2024 sur l'intérêt légitime, pt. 17 ; C-708/18, pt. 44

11. Lignes directrices 01/2019 sur la nécessité au contrat

12. C-92/09 et C-93/09

Dans tous les cas, étant donné qu’il existe des moyens beaucoup moins intrusifs pour réaliser la finalité visée par les Responsables de Traitement, les pixels traçants en sont une nouvelle fois *de facto* illicites, surtout s’ils sont utilisés sans consentement.

2.4 Sur la demande exclusive de la Personne Concernée

Au titre de la directive ePrivacy, l’exemption de consentement suppose un traitement en lien direct avec une demande expresse de la Personne Concernée ou nécessaire à une communication électronique.

Les pixels de suivi sont toujours, par nature, distincts de la communication elle-même et des services demandés par l’utilisateur.

Les bloquer n’empêche ni n’altère la communication ou la fourniture des services, à tout le moins n’est pas supposé le faire.

Aucun usage des pixels de suivi n’est donc nécessaire au sens de l’article 5(3) ePrivacy.

Une fois encore, l’usage de pixel traçant sans consentement est donc ici totalement illicite.

2.5 Sur l’attente raisonnable d’une Personne Concernée

L’intérêt légitime n’est pas mobilisable en ce que les personnes ne sauraient raisonnablement s’attendre au suivi de leur correspondance privée¹³.

L’intérêt légitime n’est donc ici pas invocable et entraîne encore une nouvelle fois l’illicéité des pixels traçants.

Par analogie avec le courrier postal, l’invisibilité des pixels de suivi est extrêmement problématique, à l’opposé d’un courrier suivi ou recommandé qui est manifeste à ce sujet.

2.6 Sur la fragmentation de l’application du RGPD en Europe

Nous rappelons que le RGPD vise à atteindre un niveau élevé de protection des personnes par une application rigoureuse des règles¹⁴.

Il vise également une application homogène dans l’UE afin de ne pas réitérer la fragmentation issue des différentes interprétations et mises en application de la directive de 1995¹⁵.

Or, à date, aucun élément ne permet d’affirmer que les homologues de la CNIL dans les autres États-Membres de l’UE, et/ou le CEPD, et/ou la CJUE, partagent l’interprétation laxiste à laquelle se livre la CNIL dans son projet de recommandation selon laquelle les pixels de suivi dans les courriels peuvent être exemptés de consentement et relever des nécessités

13. C-621/22, §55 et lignes directrices 1/2024 du CEPD sur l’intérêt légitime, §52 et 53

14. Considérants 7 et 10 du RGPD et C-26/22, point 61

15. Considérants 9 et 10 du RGPD et C-768/21, point 38

prévues par l'article 5(3) de la directive ePrivacy. WP 118 permet même d'en douter fortement et raisonnablement.

Si elle envisageait tout de même le maintien de sa recommandation, nous demandons à la CNIL de soumettre son projet à un avis du CEPD et/ou à ses homologues, ceci afin d'éviter une fragmentation de l'application du RGPD.

* *

*

De ce qui précède découle, d'une part que les finalités mêmes visées par les pixels traçants sont illicites, puisque ne respectent pas les principes fondamentaux de loyauté, de transparence, de proportionnalité et de nécessité. **Les pixels traçants contreviennent donc à l'article 5 du RGPD.**

D'autre part, l'intérêt légitime n'est pas invocable, puisque les intérêts des Responsables de Traitement sont extrêmement flous et hypothétiques et qu'une Personne Concernée ne s'attend pas à ce type de traitement.

Il existe de plus d'autres moyens techniques pour parvenir au même résultat, mais les Responsables de Traitement refusent de les utiliser par peur de voir justement les Personnes Concernées reprendre le contrôle de leurs droits et s'opposer massivement à ces traitements.

De tels traitements ne respectent donc pas les obligations faites au titre de l'article 6(1)f du RGPD.

L'exemption de consentement est de même illicite au sens de l'article 5(3) de la directive ePrivacy, puisque le traitement ne correspond pas à une demande expresse de l'utilisateur et ne peut pas relever des nécessités prévues par ce même article.

Comme dans les autres recommandations publiées par la CNIL, notre association suspecte une nouvelle fois une collusion avec les Responsables de Traitement afin d'émettre des lignes directrices approuvant des traitements en réalité illicites mais qui en deviennent inattaquables par les Personnes Concernées à la suite d'une telle publication, les Responsables de Traitement renvoyant à celle-ci et la CNIL se refusant ensuite à la moindre étude de licéité des cas d'espèce au seul motif de l'existence de ce type de recommandation.

Au lieu de légitimer des traitements manifestement illicites, la CNIL se doit de conserver la confiance du grand-public, notamment des Personnes Concernées en ce qu'elle est nécessaire à sa Formation Restreinte qui, telle une juridiction, se doit d'inspirer confiance, indépendance et impartialité et d'ôter tout doute à ces sujets¹⁶. Adopter ce projet de recommandations irait contre ce sentiment de confiance, d'image de la CNIL comme garante de la vie privée, gardienne

16. En ce sens, arrêt CEDH Dubus contre France, points 53 et suivants

des données à caractère personnel.

Nous demandons donc à votre Commission d'abandonner totalement ce projet de recommandation, contraire à la législation en vigueur et renforçant encore une fois la défiance que peuvent avoir les Personnes Concernées à l'encontre de votre Commission, supposée au contraire les protéger.

3 SUR LE CONTENU DE LA RECOMMANDATION

3.1 Sur la pertinence des questions posées

Faisant suite aux critiques émises concernant le contexte de l'organisation de cette consultation (section 1 supra), notre association s'interroge sur la raison, le sens et la pertinence des questions posées. Elles font étonnamment écho aux motifs d'illicéité de telles mesures de suivi, comme présentés ci-avant.

De telles questions laissent à penser que les Responsables de Traitement ont été dans l'incapacité de justifier de la licéité de leurs traitements et ce sur quasiment l'ensemble des points de difficulté de tels traitements.

Il est alors incompréhensible que la CNIL poursuive encore l'étude des demandes des Responsables de Traitement au travers d'une consultation publique plutôt que de retoquer immédiatement les prétentions de ces derniers.

Les Responsables de Traitement ayant été consultés bien en amont, nous ne comprenons pas comment la société civile, le grand public, et plus particulièrement les Personnes Concernées seraient à même de pouvoir éclairer votre Commission sur ce type de sujet.

Les seules entités en capacité d'y répondre, et d'ailleurs contraint légalement de le faire pour justifier de la licéité de leurs traitements, ne semblent au contraire ne pas avoir la moindre idée des réponses à fournir.

Une nouvelle fois, le fait que notre association n'ait pas pu participer aux concertations préalables nous cause ici un grand préjudice pour mieux cerner le contexte et l'intérêt de telles questions.

3.2 Sur le périmètre technologique (§2.1)

La CNIL écrit : « *Ce projet de recommandation se limite à l'usage de pixel de suivi dans les courriels.* ».

En n'étant pas indépendantes de la technologie utilisée, les recommandations en débat risquent d'être rapidement obsolètes. Par exemple, les liens traçants de détection de clic contenus dans les courriels soulèvent les mêmes problèmes et questions.

Les lignes directrices 02/2023 du CEPD les font tout autant tomber sous le coup de l'article 5(3) de la directive ePrivacy.

Notre association souhaiterait donc que ces technologies soient tout autant intégrées à ce projet de recommandation et par conséquent interdites sans consentement.

De même pour toute autre technologie traçante poursuivant plus ou moins les mêmes objectifs, comme la prise d'empreinte par canvas HTML.

3.3 Sur les acteurs concernés (§2.2)

La CNIL retient qu'un fournisseur d'emailing (liste de diffusion, publipostage, etc.) ou d'envoi est un sous-traitant au sens du RGPD.

Néanmoins, nombre d'entre eux insèrent, par défaut, des pixels de suivi et des liens de traçage liés à un client ou à une campagne précise, pour des finalités propres et non à la demande de leur client.

Notre association a ainsi vu plusieurs Responsables de Traitement découvrir que Brevo leur impose des liens traçants et l'impossibilité de désactiver cette fonctionnalité. Ceci constitue d'ailleurs en soi un défaut de contrôle de la sous-traitance, avec le choix manifeste d'un sous-traitant sans en vérifier la conformité RGPD.

En pratique, ces sous-traitants sont donc aussi Responsables de Traitement puisqu'ils ont défini des moyens et des finalités à la place de leurs propres clients.

Ces prestataires manquent à la protection par défaut des données à caractère personnel (article 25 du RGPD), à l'information de leurs clients (autre que dans les petites lignes d'un contrat de plusieurs centaines de pages), et mettent en œuvre un traitement sans suivre les instructions de leurs clients donneurs d'ordre.

Dans ses recommandations, la CNIL devrait donc préciser que les prestataires d'emailing se doivent d'informer explicitement leurs clients, dans l'interface de commande et/ou de contrôle d'une infolettre ou d'une liste de diffusion, par exemple, et n'insérer des traceurs qu'à la demande expresse d'un client.

3.4 Sur la différence entre la directive ePrivacy et sa transposition en droit national (§3)

Nous rappelons que si l'article 82 de la loi Informatique et Liberté prévoit une exemption de consentement pour ce qui a pour finalité de « *faciliter* » une communication par voie électronique, tel n'est pas le cas de l'article 5(3) de la directive ePrivacy qui restreint cette exemption

à ce qui a pour finalité « *d'effectuer* » une communication.

Dès lors, la CNIL devrait tenir compte de cette restriction du droit communautaire dans les finalités qu'elle envisage d'exempter de consentement.

3.5 Sur les finalités exemptées de consentement (§3.2)

Les cas d'usage exposés nous semblent très flous, très certainement abusifs.

Ils nous semblent très spécifiques, comme s'ils avaient été repris des desiderata des Responsables de Traitement. Nous ne comprenons pas l'absence de catégories d'usage régies par des critères objectifs. Cela donne l'impression que le projet de recommandations a été brodé autour des demandes précises des Responsables de Traitement.

3.5.1 Sur les mesures de sécurité

Nous ne voyons pas quel usage pourrait avoir un tel pixel traçant dans ce contexte, ni en quoi il serait nécessaire à la communication ou à un service demandé expressément par un utilisateur.

Comme mentionné dans vos §2.2 et 4.2, les logiciels et fournisseurs de messagerie bloquent dorénavant bien souvent tout contenu tiers ou traçant, dont les pixels traçants.

Une telle mesure de sécurité, reposant sur des conditions trop spécifiques pour être fonctionnelle, nous semble bien trop fragile pour être efficace et supposera très probablement des moyens supplémentaires de protection, bien moins intrusifs.

Ensuite, l'absence de consentement ne signifiant pas extinction du droit d'opposition, il sera dans tous les cas nécessaires aux Responsables de Traitement de prévoir des systèmes alternatifs de sécurité, rendant encore moins pertinentes et nécessaires une telle atteinte aux droits des Personnes Concernées.

L'usage de pixels de suivi contrevient même alors *de facto* à l'article 5 du RGPD et à la minimisation des traitements, le système alternatif seul étant alors ici suffisant, sans pixel traçant.

Enfin, un faux sentiment de sécurité est susceptible de naître chez les Responsables de Traitement, ce qui nuirait à la sécurité des données à caractère personnel. Les mesures envisagées nous semblent en tout cas extrêmement fragiles alors que les Responsables de Traitement leur prêtent *a priori* au contraire bien trop d'efficacité.

Il est ici très dommageable que notre association n'ait pas été conviée à participer aux travaux préliminaires, ce qui aurait permis d'avoir des détails sur un tel usage de pixels traçants et d'apporter une expertise technique en étudiant la réalité efficacité de cette finalité, qui semble ici très fortement exagérée par les Responsables de Traitement.

En l'état votre Commission demande de se prononcer sur une finalité qui nous semble matériellement impossible à satisfaire par des pixels de suivi.

3.5.2 Sur les mesures du taux d'ouverture global

Ici aussi cette finalité nous semble matériellement impossible à réaliser, et d'autant plus selon les critères d'anonymat imposés par la CNIL.

De par les blocages réalisés par les lecteurs ou les fournisseurs de courriels, de telles statistiques sont dorénavant peu fiables et pertinentes, surtout au regard de l'intrusion importante sur la vie privée des destinataires.

Nous rappelons d'ailleurs à la CNIL que la configuration du terminal utilisateur et la possibilité d'y bloquer le suivi imposé par le Responsable de Traitement n'est pas invocable par ce dernier pour contourner l'obligation de consentement ou pour choisir une base légale licite. Pour son analyse juridique, analyse de risque ou encore AIPD, le RT doit ainsi considérer que l'utilisateur n'utilisera pas de moyen de blocage.

Ce type de statistiques est d'ailleurs d'autant moins pertinent aujourd'hui, en particulier en environnement professionnel, où les outils de sécurité (pare-feu, antivirus, IDS...) déclenchent automatiquement l'ouverture des pixels à la recherche de contenu malveillant. Ce point est d'ailleurs bien identifié par votre Commission aux §2.2 et 4.2 (préchargement des liens).

De même, les Personnes Concernées peuvent afficher la seule version texte des emails qu'elles reçoivent, ce qui est d'ailleurs aujourd'hui une préconisation de sécurité (ransomware...).

La condition de non différenciation des pixels au sein d'une même campagne est aussi difficile à réaliser en pratique. Cela ne permettrait plus de distinguer facilement l'ouverture d'un même courriel dix fois par un même destinataire de l'ouverture par dix destinataires différents d'un courriel de la campagne. L'effet sur les statistiques les rendrait encore moins pertinentes.

Il est même assez fréquent, si non bloqué par le lecteur ou le fournisseur de courriel, d'avoir plusieurs déclenchements d'un pixel traçant, par exemple en naviguant dans ses courriels, chaque ouverture redéclenchant alors le pixel.

Cette mesure du taux global apporte aussi la problématique du stockage temporaire de données non anonymisées en vue d'effectuer de la déduplication *a posteriori*, par exemple sur 7 jours glissants.

Alors que la méthode est déjà en soit très intrusive et impose un suivi individualisé, elle impose ensuite du stockage supplémentaire de données non anonymisées, dont nous savons très bien que les Responsables de Traitement n'assureront jamais correctement la sécurité.

De plus, puisque tous les pixels traçants sont nécessairement techniquement individualisés, au moins dans les premiers temps du traitement, une Personne Concernée pourra en pratique

très rarement vérifier si la finalité du traitement est une mesure d’audience globale ou une mesure individualisée de son comportement, et si la configuration de l’outil lui permet une réelle exemption de consentement. Elle devra croire sur parole le Responsable de Traitement.

Une telle situation est déjà actuellement connue avec la mesure d’audience sur le web. Les outils sont soi-disant correctement configurés et ne traitent que des données agrégées, et se réclament donc bénéficiaires de l’exemption de consentement, alors que le Responsable de Traitement n’en a en réalité rien fait et contrevient manifestement à la législation, généralement à la demande de ses équipes marketing. La Personne Concernée ne peut en tout état de cause rien vérifier de la réalité du traitement mis en œuvre.

Ceci est d’autant plus problématique que votre Commission ne traite pas réellement les plaintes sur ce sujet. Elle ne vérifie jamais la réalité des mesures techniques et organisationnelles alléguées, et transforme ainsi une obligation de configuration correcte pour se réclamer de l’exemption de consentement en une exemption de consentement « *par principe* »¹⁷.

3.5.3 Sur le périmètre des courriels

Le projet de recommandations prévoit que l’exemption de consentement « *ne peut concerner que les courriels demandés par l’utilisateur ou qui se rattachent à un service demandé par ce dernier* ».

Il nous semble que tous les courriels entrent dans cette définition à l’exception des authentiques spams.

En effet, même la prospection commerciale pour un produit ou service similaire après une vente est « rattachée » à la vente, qui a été sollicitée par l’utilisateur. La CNIL le consigne d’ailleurs dans l’encart de la page 11 du projet. Tous les emails transactionnels sont également concernés.

Nous invitons vivement la CNIL à préciser ces critères dans un sens restrictif afin d’éviter toute interprétation large des Responsables de Traitement.

Pour notre part, nous pensons que la prospection caritative ou destinée aux professionnels ou pour des produits / services similaires ne constituent pas un service expressément demandé.

3.5.4 Sur la nécessité pour la délivrabilité

Un traitement est nécessaire uniquement si sa finalité ne peut être raisonnablement atteinte de manière aussi efficace par d’autres moyens moins attentatoires aux droits fondamentaux des Personnes Concernées¹⁸.

Or, la délivrabilité peut aussi être mesurée avec, entre autres :

— le « bounce rate », le taux d’erreurs, et d’autres indicateurs purement techniques ;

17. Clôtures des réclamations n^{os} 44-51084, 44-67785, et 44-1177, par exemple.

18. C-439/19, pt. 110 ; C-708/18, pt. 47

- des indicateurs usuels tels le nombre d’abonnés à une infolettre, la hausse des ventes ou de la consultation du site web de l’entité après l’envoi d’un email de prospection (mesure d’audience exemptée de consentement) ;
- de l’échantillonnage ponctuel auprès des destinataires ;
- l’inclusion, dans les listes de diffusion ou publipostages, d’adresses emails de test établies chez les principaux fournisseurs qui seront lues par des programmes informatiques de supervision ;
- un traitement automatisé des accusés de lecture volontaires par un programme de supervision (RFC 9007).

De plus, dans le domaine du courrier postal, aucun suivi aussi intrusif et à aussi grande échelle de la délivrabilité du courrier n’a jamais été mis en place sans que cela ne pose jamais aucun problème.

Une telle mesure semble donc manifestement parfaitement abusive de la part des Responsables de Traitement qui en font une nécessité *in fine* uniquement justifiée par la seule possibilité technique.

Il s’agit même très certainement d’une dérive chronique du système, en particulier pour des motivations purement marketing et mercantiles, que de traquer très fortement les Personnes Concernées au seul motif que cela est dorénavant possible.

Aucune étude réelle sur l’utilité factuelle et l’interprétation concrète de tels indicateurs n’a jamais été réalisée, relevant en pratique d’un simple culte du cargo¹⁹, sans efficacité ni intérêt aucun. Il en est d’ailleurs de même pour les statistiques d’audience.

Ainsi, la nécessité des pixels de traçage n’est pas établie, donc l’intérêt légitime n’est pas mobilisable.

3.5.5 Sur la multiplicité des bases légales

Nous constatons que la délivrabilité peut être exemptée de consentement si elle est globale, ou non si elle est individualisée.

Une telle approche va entraîner une confusion, des traitements non-conformes, et aucune vérifiabilité pour les Personnes Concernées.

La CNIL devrait associer la finalité « délivrabilité » à une et une seule base légale.

Par ce qui précède, nous ne voyons dans tous les cas pas comment l’intérêt légitime pourrait être invoqué, et seul le strict consentement est applicable.

19. https://fr.wikipedia.org/wiki/Culte_du_cargo

3.6 Sur la réutilisation des données et l'anonymisation

Notre association ne peut que soutenir ce paragraphe, qui nécessiterait même d'être renforcé.

En effet à ce jour beaucoup trop de Responsables de Traitement se réfugient derrière l'apparent anonymat des données sans jamais étudier formellement si de telles données sont bien anonymes.

Les travaux du LINC²⁰ sont éclairants sur le sujet. Ils démontrent que la plupart des données supposées anonymes ne le sont pas réellement en pratique. Un focus sur les risques de corrélation et d'inférence mériterait d'être présent dans cette recommandation.

Nous invitons également la CNIL à exposer clairement que l'anonymisation des données à caractère personnel est un pré-requis de l'exemption de consentement, notamment pour la finalité « délivrabilité ». Ceci d'autant plus que, comme présenté auparavant, une phase de traitement nécessairement non-anonyme est impérative avant une éventuelle anonymisation des données.

3.7 Sur les modalités de recueil du consentement (§4.2)

3.7.1 Sur les modalités d'information

Le projet de recommandations ne met pas assez en évidence que, quelle que soit la base légale des pixels de suivi, intérêt légitime ou consentement, la Personne Concernée doit être informée de l'existence de ce traitement de données à caractère personnel.

La politique de confidentialité, qui référence l'ensemble des traitements mis en œuvre, nous paraît l'endroit opportun pour ajouter cette information.

Elle devrait aussi être réalisée expressément au moment de la collecte de l'adresse email de la Personne Concernée.

Ainsi, nous invitons vivement la CNIL à expliciter cela dans sa recommandation.

3.7.2 Sur la durée de rétention du refus de consentir

La CNIL préconise de mémoriser le refus de consentir « *pendant un certain laps de temps* ».

Contrairement aux bandeaux cookies qui s'affichent exclusivement suite à une action de la Personne Concernée, nous sommes ici dans une situation où cette dernière aura un rôle au contraire très passif vis-à-vis de la réception d'un courriel.

Dans le cas des pixels traçants, l'expiration de ce délai de refus de consentement sera générateur de vagues de spam visant à réclamer une nouvelle expression de consentement. Ceci d'autant plus que ces nouvelles demandes doivent bien être distinctes d'un courriel pour lequel

20. <https://linc.cnil.fr/geotrouvetous-projet-de-reidentification-par-geolocalisation>

le suivi sera ensuite sollicité.

La Personne Concernée risque ainsi de finir chaque matin avec des quantités improbables de courriels contenant une nouvelle demande de consentement.

Alors qu'une Personne Concernée ne visitant plus un site auprès duquel elle avait déjà exprimé un refus de consentement ne recevra jamais de nouvelle sollicitation sans nouvelle visite active de sa part, l'inscription à une infolettre puis le refus de consentir au traçage générera activement du trafic courriel supplémentaire tous les X temps.

Il est certain qu'à recevoir régulièrement une quantité de courriels lui demandant d'exprimer son consentement, une Personne Concernée est susceptible de finir par « consentir » de manière contrainte et forcée, au même titre qu'elle le fait déjà aujourd'hui (fatigue à l'exposition) dans le cas des bannières cookies ou des applications mobiles insistantes.

Il semble ici plus que disproportionné de limiter la durée d'un refus de consentement, les effets induits étant autrement plus importants que dans le cas plus conventionnel des bannières cookies.

3.7.3 Sur l'expression libre du consentement

Encore une fois, nous ne comprenons pas le cas d'usage concernant la lutte contre l'inscription frauduleuse à un jeu-concours

Cette finalité est très simplement réalisable par du double opt-in standard et des preuves de travail qui, à notre sens, ne relèvent pas de la présente recommandation puisque ces moyens ne sont pas traçants.

Concernant l'exfiltration d'information, nous ne comprenons pas le cas d'usage, mais nous répétons ce que nous avons écrit auparavant : un pixel de suivi est une mesure de sécurité insuffisante, pour ce cas d'usage comme pour les autres.

3.7.4 Sur la connexité

Nous rappelons que le consentement doit être spécifique²¹.

Le consentement, au premier niveau, à des finalités prétendument connexes a déjà conduit, sur le web, à des pratiques délétères où une Personne Concernée se retrouve, par exemple, à consentir, en une fois, à du test A/B et à de la publicité ciblée, alors que la connexité est extrêmement discutable et que les conséquences diffèrent (la publicité ciblée fait intervenir de nombreux acteurs, brasse davantage de données à caractère personnel, procure un gain économique...).

Par ce projet de recommandations, la CNIL s'apprête à autoriser les mêmes abus dans les courriels : la prospection commerciale par courriel pour des services / produits similaires, va

21. Article 4(11) du RGPD

servir de prétexte aux autres finalités. Nous nous opposons à toute connexité.

Le seul cas d’usage éventuellement légitime présenté par la CNIL est la prospection personnalisée, et encore à condition que l’adaptation de la fréquence d’envoi n’ait pas pour objet d’optimiser la délivrabilité. Nous nous opposons aux autres cas d’usage.

A minima, nous invitons vivement la CNIL à restreindre la connexité et les cas d’usage susceptible de la satisfaire.

3.7.5 Sur l’encart d’exemption au titre de l’article 82 de la LIL

Cet encart nous paraît ici manifestement infondé et abusif.

En effet, un pixel traçant ne peut jamais être associé formellement au destinataire mais uniquement au lecteur du courriel, qui peuvent être des entités bien différentes.

Il sera par exemple d’ailleurs rappelé à la CNIL sa délibération SAN-2020-008²² à l’encontre de Carrefour concluant qu’une URL n’est pas un mécanisme de sécurisation et qu’une telle donnée doit être considérée comme publique et accessible à tous.

Si cet encart vise des liens « techniques » comme des liens d’expression de consentement aux pixels de suivi, de réinitialisation de mot de passe ou de désabonnement d’une infolettre, ceux-ci ne nous semblent pas relever du domaine de la présente recommandation en ce qu’ils n’ont pas pour finalité d’être traçants. De même, les formulaires web (de jeu-concours) peuvent être sécurisés par des preuves de travail, par exemple.

Une fois encore, il est regrettable d’avoir à commenter une telle recommandation sans avoir aucune idée des finalités et modalités techniques pratiques associées, qui ont très certainement été présentées lors des concertations privées préparatoires.

En l’état nous ne comprenons pas la faisabilité et l’intérêt technique de ce qui est présenté et ne pouvons donc que nous opposer à cet encart.

D’autant qu’il est suffisamment large, portant sur tout « *lien utilisé pour assurer la sécurité de l’utilisateur* », pour permettre à n’importe quel Responsable de Traitement de l’utiliser pour rétorquer, à tort, à une Personne Concernée que son lien est exempté de consentement selon la CNIL, qui ne vérifiera probablement jamais la réalité du traitement suite à une plainte.

A minima, la CNIL devrait préciser et restreindre le périmètre.

3.8 Sur le retrait et la gestion du consentement (§5)

Cette partie nous semble techniquement impossible à réaliser et à elle seule invalide toute possibilité pratique d’usage licite de pixels de suivi.

22. <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756>

Alors que le retrait de consentement est massivement dysfonctionnel dans l'écosystème des bannières cookies²³, nous sommes ici en face d'un objectif présentant des difficultés encore supérieures.

La CNIL soulève parfaitement la problématique du devenir des liens traçants précédemment déjà émis en cas de retrait de consentement. Les Responsables de Traitement ne pouvant pas les supprimer à distance, ceux-ci resteront éternellement actifs et traçants, là où la suppression d'un cookie garantissait (mal) une certaine purge du passé.

Les Responsables de Traitement n'auraient, dans le cas des pixels traçants, pas d'autre choix que de mettre en œuvre de nouveaux traitements de listes repoussoir afin de filtrer les déclenchements de pixels traçants concernant des Personnes Concernées ayant retiré leur consentement.

En matière de prospection commerciale, il est constant que ces listes repoussoirs sont bien trop souvent dysfonctionnelles et inefficaces en pratique²⁴. Il n'existe aucune raison de croire qu'il en irait différemment dans ce cas d'usage.

Elles présentent aussi des risques élevés pour les droits des Personnes Concernées puisqu'elles ne permettent pas l'archivage des données traitées. L'usage de simples hash des données à caractère personnel, nécessairement non salés vu la finalité visée, ne présente pas une sécurité suffisante, encore moins dans le temps, pour garantir la non réversibilité de la donnée. Il serait nécessaire de recourir à des technologies avancées (hyperloglog, filtre de Bloom, ...), technologies à notre connaissance inexistantes dans l'écosystème actuel.

Les différentes couches de Responsables de Traitement (client final, prestataire de courriel, gestionnaire d'infolettre, prestataire de statistiques), parfaitement identifiées par la CNIL, rendent aussi très complexes le suivi et l'échange des retraits de consentement.

Alors que les Personnes Concernées cherchaient au contraire à minimiser les traitements les concernant en révoquant un consentement, elles se retrouveraient dans de nouveaux traitements, pour des durées encore plus longues et dans des systèmes moins sécurisés. Le tout pour des finalités initialement déjà très discutables voire probablement illicites.

L'impossibilité technique de cette partie rend à elle seule illicite le recours aux pixels traçants puisque le consentement ne peut pas être retiré efficacement et sans effet notable sur les droits des Personnes Concernées. Elle impose l'abandon de ce projet de recommandation et l'interdiction pure et simple de ces technologies sans démonstration forte de la faisabilité et de l'efficacité d'un tel retrait.

En tout état de cause, la CNIL doit suspendre la publication de cette recommandation en l'absence d'élément probant de faisabilité technique de ce retrait.

23. Voir, par exemple, les réclamations dans lesquelles notre association est mandataire : n°s 44-94263, 44-94234, 44-94272, 44-94273, 44-94280, 44-94282, 44-94284, 44-94287, 44-99803, 44-101265...

24. Voir en cela la plainte n° 44-42208 contre Bouygues Télécom ou le recours n° 497392 devant le Conseil d'État référençant de multiples manquements et plaintes à l'encontre de Décathlon

3.9 Sur l'opposition

Concernant les finalités reposant sur l'intérêt légitime, les recommandations devraient rappeler que l'opposition au traitement est toujours possible.

Les recommandations devraient également contenir une obligation de permettre à une Personne Concernée de s'opposer par un mécanisme automatique tel un lien dans le pied de page des courriels, lors de la collecte de l'adresse email, dans la politique de confidentialité. . .

Pour les finalités exposées dans le projet de recommandation, un Responsable de Traitement ne pourra jamais se prévaloir d'un quelconque intérêt impérieux, d'autant plus encore une fois avec des finalités aussi frivoles que celles envisagées.

3.9.1 Sur l'automatisation de l'opposition

Les courriels contenant les pixels de suivi feront suite à une démarche de l'utilisateur qui se sera déroulée en ligne. Cette démarche sera très souvent automatisée (inscription à une infolettre, achat. . .).

Dès lors, l'opposition doit être automatisée au titre du considérant 59 du RGPD. La CNIL devrait l'imposer dans sa recommandation.

3.9.2 Sur les moyens techniques d'opposition

Un même email peut contenir plusieurs versions du message. En général, les emails contiennent une version HTML et une version texte. Les pixels de suivi sont absents de la version texte ou forcément inertes. Les liens de traçage demeurent et sont toujours actifs.

En l'absence de version texte dans un email, les logiciels de messagerie peuvent afficher uniquement le texte de la version HTML.

Une Personne Concernée qui affiche ses emails en version texte peut être perçue comme refusant le traçage, à l'instar de celle activant Do Not Track ou Global Privacy Control²⁵. Cette opposition est prévue à l'article 82 Informatique et Libertés :

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

De plus en plus souvent, les Responsables de Traitement (commerçants, Caisse nationale des allocations familiales, MailInBlack. . .) insèrent, dans leurs courriels, une version texte vide, ou incohérente avec la version HTML, ou renvoyant vers une version web du courrier (version qui contient elle-même des traceurs).

25. <https://globalprivacycontrol.org/>

Dès lors, les logiciels de messagerie configurés pour n’afficher que du texte, n’affichent plus le texte de la version HTML, mais la version texte, qui ne porte aucune signification.

Dans ses recommandations, la CNIL devrait imposer que tout courriel comprenant un pixel de suivi ou des liens de traçage contienne également une version texte fonctionnelle et dénuée de lien de traçage.

La CNIL devrait aussi imposer aux Responsables de Traitement la prise en compte de mécanisme de notification d’opposition tel que le Global Privacy Control.

La présence de ces signaux dans les requêtes de pistage, correspondant à une opposition à ce type de traitement, doit nécessairement désactiver tout traitement de suivi.

La CNIL devrait conditionner l’usage de pixel ou de lien traçant, et l’exemption de consentement associée, à la prise en compte obligatoire de ces signaux d’opposition.

3.10 Sur le défaut d’instruction de la CNIL

Il sera rappelé que votre Commission refuse de se saisir correctement des violations qui lui sont soumises en prétextant la seule existence de recommandations pour ne pas sanctionner les Responsables de Traitement. Elle considère en effet que « *par principe* » l’existence d’une recommandation suffit à garantir que tous les traitements sont licites et correctement mis en œuvre.

Elle ne vérifie à aucun moment l’ensemble des conditions **nécessaires et cumulatives** pour atteindre une éventuelle licéité et les remplace à chaque fois par une unique condition **suffisante** de simple et seule existence d’une recommandation.

Nous sommes déjà confrontés massivement à ce problème en ce qui concerne les bannières cookies ou l’exemption de consentement pour la mesure d’audience web ²⁶.

La seule constatation d’un bouton « Continuer sans accepter » ou l’usage d’un des outils de mesure d’audience approuvés par la CNIL entraînent immédiatement la clôture des réclamations sans réelle étude, par exemple, de la nécessité des traitements, de la configuration réelle des outils de mesure audience ou de l’effectivité du droit d’opposition ou du retrait de consentement.

Si votre Commission envisage le maintien de cette recommandation sur les pixels traçants, nous demandons une refonte complète du processus d’instruction des réclamations par la CNIL. Ceci afin d’avoir une réelle application des recommandations en vigueur et à venir et une véritable protection des droits des Personnes Concernées.

En l’état, la plupart des recommandations de la CNIL ne visent en pratique qu’à défendre les intérêts des Responsables de Traitement et à l’extinction des droits des Personnes Concernées.

Le peu d’éléments éventuellement protecteurs, comme une obligation de configuration correcte des outils de mesure d’audience exemptés de consentement, ne sont en pratique jamais

26. Réclamations 44-51084, 44-67785, et 44-1177, 44-94263, 44-94234, 44-94272, 44-94273, 44-94280, 44-94282, 44-94284, 44-94287, 44-99803, 44-101265, etc.

vérifiés ni mis en œuvre par la CNIL.

Il en sera manifestement de même avec cette recommandation sur les pixels traçants, la CNIL n'ira jamais s'assurer de la conformité réelle des Responsables de Traitement, qui seront en capacité de ne pas respecter les obligations pourtant présentes.

Aujourd'hui, les recommandations déjà existantes ne sont même pas respectées par la CNIL elle-même et ses équipes d'instruction des réclamations. Nous ne voulons pas voir une nouvelle recommandation dans cette situation.

Nous demandons donc une profonde refonte des procédures d'instruction des réclamations de la CNIL avant toute publication de nouvelles recommandations.

4 CONCLUSION

Par tout ce qui précède, notre association s’oppose très fortement à la publication d’une telle recommandation par la CNIL, qui n’a pour vocation que de maintenir des traitements manifestement contraires à la législation en vigueur.

Ce type de traitement est au contraire illicite et ce à de multiples égards (article 5 et 6 RGPD, article 5(3) ePrivacy, ...)

Nous demandons l’abandon pur et simple de ce projet de recommandation et l’interdiction formelle de ces pixels et liens traçants sans strict consentement.

Nous demandons au moins la suspension de la publication de cette recommandation

- jusqu’à la démonstration formelle de la réalité, de l’intérêt, de l’utilité et de l’efficacité des finalités visées, en particulier au regard du blocage des pixels traçants et de l’ouverture automatique par les antivirus et IDS ;
- jusqu’à ce que les Responsables de Traitement apportent des solutions techniques réelles et concrètes, aujourd’hui totalement inexistantes, aux graves problèmes d’intrusion dans la correspondance privée des Personnes Concernées, en particulier en ce qui concerne la prise en compte correcte et effective d’un retrait de consentement ;
- jusqu’à la refonte des services d’instructions de la CNIL de manière à être en capacité réelle de faire appliquer la législation en vigueur et les recommandations publiées, ce qui n’est pas le cas aujourd’hui.

En cas de maintien de ces travaux, nous demandons l’ajout de l’ensemble des garanties fortes sus-mentionnées concernant la protection des droits des Personnes Concernées, une restriction drastique des conditions d’exemption de consentement (et une réelle vérification de celles-ci par la CNIL en cas de réclamation), ceci pour éviter toute dérive, ainsi qu’une réelle prise en compte du droit d’information et d’opposition.

D’ores et déjà, nous invitons vivement la CNIL à organiser ses services d’instruction des plaintes pour être en capacité d’étudier correctement les conditions d’exemption, l’obligation de minimisation de traitement, les obligations entourant l’intérêt légitime, l’obligation d’encadrement de la sous-traitance, etc., qui sont autant de conditions **cumulatives** de licéité, que la CNIL refuse toujours de considérer lorsqu’une réclamation en ce sens lui est soumise.

Pour l'association PURR,
Son Conseil d'administration



« aeris »

