



Projet de recommandation relative aux pixels de suivi dans les courriers électroniques – CNIL

Contribution à la consultation publique et au questionnaire économique

Alliance Digitale

Introduction

Alliance Digitale est la principale association professionnelle des acteurs du data et du marketing digital en France. Elle est issue du rapprochement de l'IAB France, de la Mobile Marketing Association France et de la DMA Data Marketing Association France. L'association représente l'ensemble des professions et professionnels liés à la data et au marketing digital en France, soit près de **300 entreprises réparties sur l'ensemble de la chaîne de valeur** – agences médias et conseils, éditeurs et régies, acteurs de la logistique, data providers, fournisseurs de solutions Tech (adtech, martech) et marques.

Alliance Digitale rassemble parmi ses membres de nombreux fournisseurs de solutions de campagnes et de pixels de suivi, ainsi que des entreprises qui en sont clientes. **Alliance Digitale a donc vocation à répondre à l'ensemble des éléments couverts par le projet de recommandation et le questionnaire économique mis en consultation par la CNIL.**

Tout d'abord, **nous accueillons favorablement cette démarche de la CNIL visant à aider les professionnels dans leurs démarches de mise en conformité.** Alliance Digitale s'est mobilisée depuis le début des travaux initiés sur ce sujet, notamment en participant aux différents ateliers organisés par la CNIL en 2024.

Nous regrettons néanmoins que l'essentiel des points que nous avons partagés lors de cette phase préalable soit absent dudit projet de recommandation. Nous espérons que la version publiée tiendra compte des problématiques juridiques, techniques et économiques identifiées par le secteur, qui découlent des impacts importants que le projet aurait, en l'état, sur tous les acteurs et utilisateurs.

La contribution de l'Alliance Digitale traite d'abord du projet de recommandation, en formulant des **remarques générales puis spécifiques** suivant l'organisation de ce document. Puis, les premiers éléments partagés par nos membres viennent nourrir les questions posées dans le cadre du **questionnaire économique.**

1. Synthèse et recommandations

Ce projet de recommandation soulève de nombreuses interrogations et inquiétudes pour l'ensemble des membres de l'Alliance Digitale. Dans cette réponse à la consultation publique, **nous alertons la CNIL principalement sur :**

- **Le besoin de coordination européenne sur ce sujet :** cette recommandation n'a pas d'équivalent à notre connaissance dans d'autres pays membres, créant ainsi une spécificité française ;
- **Le manque de prise en compte à la fois de la valeur très importante** qu'apportent les pixels à tous les acteurs et in fine, aux utilisateurs, **et du fort impact économique** que les recommandations soumises à consultation auraient sur le secteur, avec des **risques de mise en danger des obligations légales qui s'imposent également** aux entreprises ;
- **L'absence de distinction entre les différents usages techniques des pixels :** le projet ne différencie pas suffisamment les traitements strictement nécessaires à la sécurité ou à la délivrabilité, de ceux à visée de personnalisation ou de profilage marketing ;
- **La nécessité d'avoir une période d'adaptation d'au moins 6 mois**, compte tenu des nombreux développements qui devront être faits pour la mise en conformité ;
- **La rétroactivité de ce projet**, qui s'appliquerait en l'état aux bases de données déjà constituées : cela mettrait en risque la sécurité juridique des entreprises ;
- **Les développements sur l'anonymisation des données**, alors même que le CEPD n'a pas encore publié de lignes directrices et qu'une décision européenne est attendue prochainement sur le sujet.

Pour la publication définitive, nous recommandons à la CNIL de :

- **Présenter un avant-projet de recommandation avant toute phase de concertation :** cela permettra de travailler sur une base connue de toutes les parties prenantes ;
- **Privilégier une approche souple dans l'interprétation de la directive ePrivacy, dont l'applicabilité aux pixels de suivi reste toujours à démontrer ;**
- **Préciser un certain nombre de termes** dans la future recommandation, comme « *service demandé par l'utilisateur* », « *finalités fortement connexes* », etc. ;
- **Permettre aux entreprises de regrouper les finalités**, en cohérence avec ce qui relève d'opérations de traitement de ce qui est un objectif auquel ils concourent ;
- **Laisser de la flexibilité aux entreprises dans les modalités techniques** de recueil du consentement, en évitant une approche prescriptive ;
- **Aligner les modalités de refus et d'acceptation du consentement**, comme pour les cookies (retrait et acceptation aussi simple) ;
- **Unifier les règles de conservation de la preuve de consentement cookies et pixels ;**
- **Prévoir la même base légale pour les pixels de suivi et pour l'envoi de campagnes de courriels :** cela permettrait de tenir compte des difficultés engendrées par la demande d'un consentement pour les utilisateurs dont les données personnelles ont été collectées légitimement sur une base légale autre ;
- **Supprimer les développements sur le retrait des pixels de suivi dans les courriels déjà envoyés après retrait du consentement :** cela est techniquement impossible et créerait les conditions de la non-conformité ;
- **Supprimer les développements sur les liens traçants :** ceux-ci n'ayant pas été expertisés lors de la concertation, leur inclusion ici ne se justifie pas.

2. Remarques générales

En préambule, nous tenons à saluer la **publication de ce projet de recommandation après celui des lignes directrices du Comité européen de la protection des données (CEPD)**. Son **ouverture à commentaires**, après une phase de concertation, est également positive en ce qu'elle donne une opportunité supplémentaire aux acteurs d'apporter leur expertise.

Ce projet de recommandation suscite quatre grands types de remarques. Celles-ci portent sur (1.1) les conditions d'élaboration de ce projet, (1.2) l'opportunité de préciser la directive ePrivacy, (1.3) l'impact économique de ce projet qui apparaît disproportionné par rapport au gain qu'en retireraient les utilisateurs et (1.4) la faisabilité technique des propositions de la CNIL concernant l'après retrait du consentement.

2.1. *Sur les conditions d'élaboration de ce projet*

Afin de rédiger son projet de recommandation, la CNIL a organisé 4 ateliers au cours de l'année 2024. Ceux-ci ont permis de réunir des acteurs divers et complémentaires pour échanger sur l'utilisation des pixels de suivi. Lors de ceux-ci, nous avons formulé de nombreuses propositions dont nous regrettons qu'elles n'aient été que **très peu reprises** ici. De plus, ces ateliers ont été menés sur la base de questionnaires et non d'un projet de recommandation. La CNIL a su dans d'autres types de concertations communiquer très en amont aux acteurs quelles étaient ses pistes de travail, comme dans le cadre de la consultation sur le consentement multi-terminaux¹. **Pour le futur, nous recommandons donc que soit partagé un avant-projet de recommandation dès le début des concertations afin de clarifier les éléments ainsi évalués par la CNIL.** Cela permettra à tous les acteurs d'y contribuer avec les éléments techniques appropriés, engageant ainsi un dialogue sur une base connue de toutes les parties. **Sans cela, il est à craindre que l'utilité de la concertation soit perçue comme très faible.**

Il est également important de relever qu'à notre connaissance, ce travail ne trouve pas d'équivalent dans d'autres pays membres de l'Union européenne. Sans coordination au niveau européen via le CEPD, cette recommandation va donc créer une spécificité nationale. Les effets pourraient être double : distorsions de concurrence entre sociétés françaises soumises à cette recommandation et entreprises d'autres pays européens, risques de délocalisations vers d'autres géographies. De plus, selon les pays membres, l'application de la directive vie privée et communications électroniques (« directive ePrivacy ») n'est pas toujours du ressort d'une autorité de protection des données, ce qui peut impliquer des interprétations très différentes des lignes directrices du CEPD. **Une coordination européenne nous semble donc nécessaire. Elle permettrait également de renforcer davantage le marché unique du numérique.**

Si la CNIL devait néanmoins poursuivre dans cette voie et publier sa recommandation, un délai d'adaptation d'au moins 6 mois nous semble nécessaire compte tenu des nombreux investissements que les entreprises devront engagés et qui sont détaillés dans la suite de cette réponse.

¹ « Consentement multi-terminaux : la CNIL lance une consultation publique sur son projet de recommandation », CNIL, 24 avril 2025. URL : <https://www.cnil.fr/fr/consentement-multiterminaux-consultation-sur-le-projet-de-recommandation>

2.2. Sur l'opportunité de préciser la directive ePrivacy

Nous nous interrogeons également sur l'utilité même de préciser la directive ePrivacy. **Cette directive est en effet de plus en plus questionnée** et pourrait même faire l'objet de futures propositions de simplification de la part de la Commission européenne². Le projet de *Data European Union Strategy* de la Commission envisage par ailleurs d'alléger la charge du consentement. Le régulateur des données personnelles britannique, qui s'appuie sur une réglementation calquée sur cette directive, a de son côté lancé une consultation publique afin d'identifier les activités publicitaires qui pourraient faire l'objet d'une souplesse réglementaire³. Cette concertation fait suite à la publication d'un plan d'action en début d'année par le régulateur sur les activités considérées comme posant peu de risques au regard de la protection des données personnelles⁴.

Nous recommandons une **approche à la fois souple dans l'interprétation de la directive ePrivacy et qui tient compte de ses nombreuses interactions avec les législations existantes** :

- avec le règlement général sur la protection des données (RGPD) : par cohérence avec la base légale pour les traitements subséquents de données personnelles, une exemption de consentement pour les pixels de détection de la fraude pourrait être prévue ;
- et avec le code des postes et des communications électroniques (CPCE) : une articulation entre l'article 34-5 qui autorise la prospection directe sans consentement supplémentaire si celle-ci concerne « *des produits ou services analogues* » et une exemption de consentement pour les pixels dans des courriels dans le même cadre pourrait aussi être prévue.

La clarification de ces différentes interactions par le régulateur constituerait un apport bienvenu pour le secteur dans sa mise en conformité.

Enfin, depuis l'adoption de la directive ePrivacy, le fonctionnement technique du protocole TCP/IP n'a pas évolué de manière substantielle. Les « données émises », qui n'était pas considérés comme étant stockées dans le terminal alors, ne peuvent se justifier comme le devenant aujourd'hui. De plus, cette directive avait vocation à encadrer ce type de données, explicitement reconnues comme étant hors de son périmètre d'application. Enfin, il n'a toujours pas été prouvé techniquement que l'utilisation de pixels de suivi revient à un accès en lecture et/ou écriture sur le terminal de l'utilisateur comme le prévoit l'article 82 de la loi Informatique et Libertés qui transpose l'article 5(3) de la directive ePrivacy. **L'applicabilité de la directive aux pixels de suivi est donc fondamentalement problématique.**

² Par exemple, en marge du Conseil Télécommunications du 6 juin 2025, la présidence polonaise a présenté un rapport sur les résultats des discussions avec l'industrie du numérique tout au long de sa présidence sur le sujet de la simplification. Dans celui-ci, elle recommande notamment d'instaurer de nouvelles obligations légales communes pour tous les régulateurs et la Commission européenne afin qu'ils prennent en compte l'impact de la réglementation et de son application sur la compétitivité, l'innovation et la croissance (URL : <https://data.consilium.europa.eu/doc/document/ST-9383-2025-INIT/en/pdf>).

³ « ICO call for views on our approach to regulating online advertising », Information Commissioner's Office (ICO), 7 juillet 2025. URL : <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/07/ico-call-for-views-on-our-approach-to-regulating-online-advertising/>

⁴ « Online tracking strategy », Information Commissioner's Office (ICO), 2025. URL : <https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/online-tracking-strategy-1/>

2.3. *Sur l'absence de proportionnalité entre l'impact économique de ce projet et le gain qu'en retireraient les utilisateurs*

Ce projet de recommandation de la CNIL applique des règles uniformes à tous les acteurs (associations, entreprises, brokers, etc.) et à tous les types de courriels (transactionnels, informationnels, marketing), **sans distinction de leur finalité, du type de destinataires adressés (BtoB ou BtoC) ou encore de leur impact**. Cette uniformité ne permet pas de prendre en compte la variété des utilisations actuelles des pixels de suivi.

En particulier, **le projet de recommandation ne prend pas assez en compte la valeur très importante qu'apportent les pixels de suivi**. Ils permettent notamment d'assurer que les campagnes atteignent leurs destinataires et de respecter ainsi les filtres mis en place par les fournisseurs de messagerie (**délivrabilité**). Un moindre usage des pixels de suivi conduirait nécessairement à une **hygiène des bases** plus basse et à sur-solliciter les utilisateurs. Les risques de voir sa **réputation** en tant qu'annonceur et routeur de campagnes dépréciée par les fournisseurs de messagerie, avec des effets par exemple sur les stratégies de chauffe des IP⁵ et la capacité à envoyer de nouvelles campagnes, sont réels.

Par ailleurs, la gestion de bases mêlant utilisateurs ayant accepté et ceux ayant refusé l'usage de pixels de suivi représentera un **développement technique** nouveau, et donc autant de ressources financières et humaines à mobiliser pour les entreprises. Celles-ci ne pourront pas en effet se reposer uniquement sur les indicateurs qui font l'objet d'exemption de consentement dans le projet de recommandation. Les taux d'ouverture globaux montrent un engagement mais ne permettent pas d'améliorer la diffusion, tandis que les taux de clics sont très faibles dans une campagne et ne peuvent pas non plus suffire pour savoir si une personne est intéressée ou non par ces envois. Il est également à noter que certains types de campagnes ne sont tout simplement peu ou pas cliquables, s'agissant par exemple de courriels d'information sur une commande, liée à l'actualité, etc.

De plus, le courriel est l'un des seuls moyens de communication non-intermédié entre marques et clients ou prospects. La complexification de son utilisation, sans les nuances que nous avons mentionnées, pourrait conduire à un **abandon progressif de cet outil**. Il est donc à craindre une moindre innovation dans le secteur, voire le **report des budgets publicitaires** vers des acteurs basés à l'étranger et n'apportant pas les garanties de sécurité et le même niveau de protection qu'en France. Certains de nos membres nous ont également partagé un risque de report vers des environnements fermés, ce qui accentuerait encore la concentration du marché.

2.4. *Sur la faisabilité technique des propositions concernant l'après retrait du consentement*

Le projet indique qu'afin de gérer le retrait du consentement par l'utilisateur pour l'envoi de pixels de suivi dans les courriels à venir, *« il peut être nécessaire de mettre en place des solutions spécifiques pour **garantir l'absence de lecture des traceurs précédemment utilisés** (notamment lorsque le destinataire ouvre à nouveau le courriel) pour que le retrait du consentement soit effectif »*. Aucune solution n'existe actuellement permettant une

⁵ Il est courant que les adresses IP doivent établir une réputation d'expéditeur légitime auprès des fournisseurs de messagerie avant de pouvoir envoyer une campagne, ce qui est appelé « chauffe des IP ».

suppression à distance de pixels dans des courriels déjà envoyés. Cette proposition est donc irréaliste et met de facto l'ensemble des acteurs dans une situation de non-conformité. Elle semble également confondre le droit d'opposition et le droit d'effacement, allant ainsi juridiquement plus loin que ce que prévoit le RGPD en la matière.

3. Remarques spécifiques

La présente partie formule en détail des observations sur les différents aspects couverts par le projet de recommandation. Elle en reprend l'organisation telle que soumise à consultation publique.

3.1. Introduction

Nous comprenons que le travail autour de ce projet de recommandation a été déclenchée par le dépôt d'un nombre de plaintes relativement modeste. Compte tenu des débats au niveau européen sur la possible actualisation de la directive ePrivacy mentionnés plus haut, l'impact de la future recommandation sur le secteur et du nombre important de pratiques dont il est proposé qu'elles fassent l'objet d'un consentement supplémentaire, nous recommandons à la CNIL de faire preuve de la plus grande vigilance afin de **trouver un point d'équilibre entre protection des données personnelles et mise en conformité pragmatique**.

Par ailleurs, nous notons que la CNIL ne donne un caractère « *ni réglementaire ni exhaustif* » à ce projet de recommandation, ce qui ne manque pas de poser question sur sa **valeur juridique**. Des éclaircissements sur ce point seraient particulièrement bienvenus.

3.2. Périmètre du projet de recommandation

Nous tenons tout d'abord à souligner que **l'emploi de termes comme « pixels espions » est tout à fait inapproprié**. Ce type de vocabulaire a pour effet de créer de la confusion sur des technologies dont on a déjà rappelé plus haut l'intérêt pour l'ensemble des acteurs, et in fine les utilisateurs.

Les développements consacrés aux « *qualifications au sens du RGPD* » des acteurs ne manquent pas également de nous interroger. En effet, il est fait mention de **nombreux cas dans lesquels une qualification de responsable de traitement ou de responsable de traitement conjoint est retenu**. Or il semble nécessaire de distinguer par exemple les cas dans lesquels les prestataires de services de location de listes de diffusion et d'envoi de courriels, lorsqu'ils utilisent des pixels en vue d'améliorer la qualification de leurs listes ou la délivrabilité auprès des fournisseurs de messagerie, sont seuls responsables de traitement. L'expéditeur du courriel n'est pas, dans ce cas, responsable de traitement conjoint si les informations collectées permettent d'améliorer dans leur ensemble le service proposé par ces prestataires.

3.3. Objectifs poursuivis par le traitement (finalités)

Dans ce projet de recommandation, **de nombreuses utilisations des pixels feraient l'objet de consentement supplémentaire alors même qu'elles contribuent à rendre les campagnes de courriels efficaces, ciblées et spécifiques** aux intérêts des utilisateurs.

Il en est ainsi de :

- **la mesure individuelle et l'analyse du taux d'ouverture des courriels : cet usage est l'un des plus standards dans le secteur**, y compris par des structures de taille modeste de type associatif pour lesquelles un tel indicateur leur permet de mieux cibler leurs communications, suivre le règlement des cotisations, faire des campagnes de dons, etc. Une bonne hygiène de bases de données ne peut en effet se faire qu'à l'aide de cette mesure individuelle. Elle permet de ne solliciter que les utilisateurs intéressés, préservant ainsi leur tranquillité et réduisant l'impact environnemental des campagnes qui bénéficient ainsi d'un ciblage approprié. Il est donc à craindre qu'un moindre usage du pixel ne permette plus un tel suivi, et donc entraîne un envoi beaucoup plus important de courriels sans cette capacité à les différencier selon l'activité des destinataires ;
- **la détection et l'analyse de suspicions de fraude** : par nature, des utilisateurs malveillants ne consentiront pas à l'utilisation de pixels de suivi dans les courriels qui pourraient leur être envoyés. La capacité par exemple à détecter qu'un courriel a été ouvert à de nombreuses reprises, qui peut relever d'une automatisation depuis un compte frauduleux, doit être préservée au risque sinon de priver les acteurs de la campagne d'outils utiles à la prévention et à la lutte contre la fraude.

Au rang des **finalités exemptées du recueil de consentement** dans le projet de recommandation, nous relevons également que :

- **les « service[s] demandé[s] » par les utilisateurs ne bénéficient d'une exemption de consentement que pour la mesure du taux global d'ouverture des courriels** : ces services demandés devraient faire l'objet d'une exemption au titre de la mesure individuelle et pas uniquement des liens traçants comme l'encadré en partie 4 l'indique. Ils peuvent par exemple émaner d'organismes clés (Gouvernement, ministères, DGFIP, services de police et de gendarmerie, administrations de santé, services liés à la gestion des pensions, hôpitaux, etc.) ou venant en confirmation d'un service souscrit par l'utilisateur (confirmation de rendez-vous, de commande, etc.) ;
- **en conséquence, l'utilisation des pixels de suivi pour faire respecter des obligations contractuelles est mise en risque** : c'est par exemple le cas des renouvellements tacites de contrat, de ceux reposant sur un principe de recommandé similaire au recommandé postal comme une confirmation de réception d'une information ou d'un colis, etc. Des exemptions pour ce type de cas devraient donc également être prévues par la CNIL pour ne pas affecter le respect par les entreprises de leurs obligations légales ;
- **de plus, la seule exemption prévue pour la finalité de lutte contre la fraude concerne l'authentification de l'utilisateur** : l'exemple donné est celui d'un courriel de réinitialisation de mot de passe. Or il faut relever que la lutte contre la fraude concerne toute mesure de sécurisation des canaux de communication, et pas uniquement dans le cas cité. Une clarification de ce passage semble nécessaire ici.

Enfin, il est fait mention d'une **exemption en cas de réutilisation de données « à la condition qu'elles aient été préalablement anonymisées de manière effective »**. En l'absence de critères existants en la matière et dans l'attente de lignes directrices du CEPD sur le sujet qui devraient prendre en compte la future décision dans le cas *European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB)*, ce point préempte la publication de nouveaux instruments de droit souple et de décisions européennes. Cela contribue là aussi à créer une spécificité française, qui pourrait de plus devenir rapidement caduque.

3.4. *Information et consentement*

3.4.1. Information sur les finalités des traceurs

La CNIL recommande la mise en avant de chaque finalité avec un descriptif d'accompagnement, en donnant de nombreux exemples. Or ces derniers relèvent d'opérations de traitement et non de finalité, celle-ci se définissant comme l'ensemble des opérations de traitement y concourant. **Nous recommandons ici de s'en tenir à une finalité** (prospection commerciale par voie électronique) **ou deux** (publicité personnalisée ou non-personnalisée) afin de gagner en cohérence.

De plus, la multiplication de tels choix en premier niveau d'information concourt à une **« fatigue du consentement » pour l'utilisateur, sans apporter d'informations essentielles pour éclairer son choix**, ce qui risque de faire baisser le taux de consentement. En cas de collecte via un tiers, la complexité sera encore plus grande car il sera nécessaire d'obtenir un consentement pour l'envoi de courriels et un autre pour l'inclusion de pixels de suivi dans ces mêmes courriels, avec potentiellement des tiers différents pour chacun de ces consentements.

Concernant plus particulièrement l'exemple donné de **« création de profils des destinataires »**, il s'agit d'une opération de traitement pour réaliser ensuite de la publicité ou de la prospection commerciale personnalisée ou non-personnalisée. Celle-ci doit impérativement être placée au bon niveau d'information, avec en première instance la ou les finalités mentionnées précédemment et via un ou deux boutons de déroulement, le détail des opérations.

Par ailleurs, la CNIL recommande dans tous les exemples donnés de citer les **sociétés tierces**. Cette mention ne semble justifiable que si celles-ci sont responsables de traitement, et non simples destinataires (cf. partie 3.2. de notre réponse).

Enfin, le développement du projet de recommandation concernant la **« description plus détaillée de ces finalités »** qui devrait être **« aisément accessible depuis l'interface de recueil du consentement »**, semble indiquer que la CNIL souhaite que les plateformes de gestion du consentement (CMP) soient utilisées pour ce recueil. Or dans la partie suivante (4.2), la CNIL recommande le recueil du consentement lors de la collecte de l'adresse électronique, ce qui se rapproche davantage d'un recueil par case à cocher. Ce type de prescription peut entrer en conflit avec des systèmes qui ne communiquent pas à ce stade ou même ne pas permettre de répondre à des besoins liés à différents types de communication : données propriétaires ou transmises par des tiers, BtoB ou BtoC, etc. De plus, cette rédaction qui pointe alternativement des mécanismes de consentement différents ne devrait pas impliquer nécessairement la mise en place à la fois d'une CMP et d'un consentement (opt-in) prospection commerciale, afin lorsque cela est possible de pouvoir simplifier le recueil du consentement. **Il nous semble donc**

important que les acteurs aient le choix dans les modes de recueillement, et ce afin de leur permettre d'utiliser la solution technique adéquate.

3.4.2. Modalités pratiques de recueil du consentement

La CNIL recommande d'intégrer une « *information synthétique sur les finalités des traceurs... avec un lien vers une information plus détaillée* ». Comme indiqué plus haut, nous recommandons plutôt d'avoir un groupement sous une ou deux finalités et qu'un bouton de déroulement permette à l'utilisateur de prendre connaissance des détails concernant celles-ci, avec d'éventuels liens vers des informations plus détaillées.

Le projet de recommandation indique également que dans certaines conditions, le recueil d'un consentement valide pour les pixels de suivi peut être difficile « *par exemple lorsque l'adresse est recueillie à l'oral* ». Nous nous questionnons sur cette analyse, un consentement oral pouvant tout à fait être valable, et les raisons de l'inclusion de cet exemple dans ce projet de recommandation.

Par ailleurs, le projet actuel prévoit que l'ensemble des bases déjà constituées devront faire l'objet d'un nouveau consentement au titre de l'utilisation des pixels. Un **principe de non-rétroactivité** devrait ici plutôt prévaloir – au risque sinon de mettre en danger la sécurité juridique nécessaire aux entreprises. De manière pratique, si la rétroactivité était entérinée dans la recommandation publiée par la CNIL, des millions de personnes ayant consenti à recevoir des courriels vont devoir être sollicitées de nouveau, participant de la « fatigue du consentement » déjà évoquée. Certains acteurs s'attendent à un taux de consentement très bas⁶. Cela n'est pas nécessairement synonyme de désintérêt total des personnes pour la personnalisation des courriels : il pourrait également s'agir de personnes inactives, dont la suppression est de toute façon une nécessité légale et économique pour assurer une bonne hygiène de la base. Le projet actuel ne permettra plus de faire cette distinction, faisant perdre en finesse l'analyse des attentes des utilisateurs, au détriment de la délivrabilité, avec les risques de sanction par les fournisseurs de messagerie en cas de variations volumétriques des envois que cela emporte, et de la sollicitation juste des personnes (cf. point 2.3 de cette réponse).

Ce point est d'autant plus problématique concernant les **données personnelles qui ont été collectées légitimement sur une base légale autre que le consentement**, par exemple à des fins de prospection commerciale à destination de professionnels ou pour des courriels envoyés à des fins non-commerciales dans le secteur caritatif. En effet, il semble difficile d'obtenir un consentement notamment a posteriori pour des données personnelles collectées sur la base de l'intérêt légitime pour l'envoi de communications par voie électronique. En cas de collecte par un tiers, comme déjà indiqué plus haut, ou bien via des sources publiques comme la base INPI, la complexité serait encore plus grande. Cette situation serait d'autant plus complexe dans un contexte de collecte indirecte de données. **Nous recommandons ici de prévoir la même base légale pour les pixels de suivi et pour l'envoi de campagnes de courriels**, comme cela est d'ailleurs prévu au sein du référentiel de la CNIL relatif aux

⁶ Les estimations qui nous ont été partagées oscillent entre moins de 1 % et 5 % de consentement d'une base de données déjà constituée. Pour les nouveaux clients ou prospects, le taux de consentement dépendra également de la manière de le recueillir. A titre d'exemple, les CMP cookies favorisent plutôt l'acceptation et le taux moyen de consentement y est d'environ 30 %. Il est à craindre que ce chiffre pour les pixels soit bien en-deçà.

traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales, pour la transmission de données personnelles à des fins de prospection commerciale.

Les développements concernant les **liens traçants**, qui font l'objet d'un encadré spécifique dans ce projet de recommandation, nous interrogent également. Ceux-ci n'ont pas été discutés dans le cadre des ateliers de concertation menés par la CNIL et l'analyse ayant conduit à les faire apparaître n'a pas été partagée au préalable. Leur inclusion dans le champ de la directive ePrivacy est quoi qu'il en soit questionnable. Comme pour les pixels de suivi (cf. partie 2.2 de notre réponse), à ce jour l'accès en lecture et/ou écriture sur le terminal de l'utilisateur que permettraient ces liens n'est toujours pas prouvé.

Il est par la suite mentionné que l'enregistrement des choix des destinataires doit permettre de ne plus les solliciter dans les courriels ultérieurs « **pendant un certain laps de temps** ». Il nous semblerait utile que la CNIL précise ses attentes en la matière. Les futures procédures à mettre en place par les entreprises afin d'être en conformité seront ainsi plus sécurisées juridiquement.

La CNIL indique également qu'un **recueil de consentement unique dans le cadre d'un couplage de finalités** est « *susceptible d'affecter, dans certains cas, la liberté de choix et donc la validité du consentement* ». Il est par la suite précisé que peuvent être regroupées des « *familles de finalités fortement connexes* ». Ces termes gagneraient à être précisés, car ils occasionneront sinon des confusions et interprétations divergentes.

Après les exemples de couplage de finalités donnés, nous nous interrogeons également sur le paragraphe mentionnant que **la publicité display et la prospection commerciale sont « deux finalités distinctes »**. Or la prospection commerciale peut avoir un objectif publicitaire. Nous rappelons par ailleurs que la finalité publicité *display* fait déjà l'objet d'une base légale au sens du RGPD.

3.5. Retrait et gestion du consentement

Nous constatons une **asymétrie entre les actions nécessaires pour donner un consentement** (deux clics recommandés par ce projet) **et l'unique action recommandée** pour refuser le pixel de suivi. Cette situation n'est pas justifiée notamment par parallélisme avec le régime applicable aux cookies, pour lesquels « *il doit être aussi simple de retirer son consentement que de le donner* »⁷. Elle semble par ailleurs exclure la gestion des consentements directement depuis un espace client, où sont centralisées nombre de ces informations, ce qui risque de rendre illisible la situation pour l'utilisateur. Sur ce dernier point, nous prôtons une approche plus souple comme exposé précédemment (cf. partie 3.4.1 de notre réponse).

Par ailleurs, une situation n'est pas couverte par la CNIL : comment gérer le **désabonnement de l'envoi de courriels par un utilisateur, qui aurait précédemment consenti à l'envoi de pixels de suivi, puis son réabonnement** à ceux-ci ? Le consentement au pixel est-il toujours

⁷ « Cookies et traceurs : que dit la loi ? », CNIL, 29 septembre 2020, page consultée en juillet 2025. URL : <https://www.cnil.fr/fr/cookies-et-autres-traceurs/que-dit-la-loi#:~:text=Le%20consentement%20doit%20pouvoir%20être,la%20disposition%20de%20l'utilisateur.>

valide, puisque le retrait puis le nouveau consentement ne concernait que l'envoi de courriels ? Ce type de situation est loin d'être anecdotique. Sans précision supplémentaire, un flou entourera la mise en conformité à la future recommandation.

3.6. *Preuve du consentement*

La gestion de la preuve du consentement aux pixels de suivi dans les courriels – hébergement, mise à jour, utilisation dans le cadre des campagnes à venir, etc. – est une problématique nouvelle pour le secteur. Elle ne s'appuie pas comme dans d'autres cas comme les cookies sur des standards déjà existants. De plus, dans le cas des cookies c'est une preuve de procédé qui est requise et non individualisée. Il serait donc utile à notre sens qu'une **vision unifiée des deux régimes** soit adoptée par la CNIL.

Par ailleurs, la CNIL devrait préciser le **périmètre** de cette obligation, la **durée de conservation** recommandée, et **confirmer la pertinence de mécanismes déjà existants**, comme des logs systèmes attestant du statut du consentement d'une liste d'envoi à un instant donné.

Si la vision unifiée des régimes que nous préconisons n'est pas retenue, cela demandera des investissements dédiés. Si le ratio coûts/bénéfices apparaît positif malgré les remarques et constats que nous avons déjà dressés, ces investissements ne pourront pas donner de résultats de manière immédiate et un délai d'adaptation sera nécessaire (cf. 2.1 de notre réponse).

4. Questionnaire économique

Les éléments ci-dessous sont les premiers chiffres et analyses communiqués par nos membres. L'analyse de l'impact économique du projet de recommandation requiert la mobilisation d'équipes différentes et la construction de scénarios nouveaux. Ils ne sont donc pas exhaustifs et pourraient être complétés par la suite.

Question 1 : Le taux d'ouverture est-il un indicateur pertinent pour mesurer la délivrabilité des e-mails, notamment eu égard à son biais potentiel du fait de l'impact de l'Apple Mail Privacy Protection (MPP), par rapport à d'autres indicateurs (CTR, bounce rate, etc.) ?

Certains de nos membres nous ont partagé les éléments suivants :

- tout d'abord, il faut rappeler que **la part de marché des systèmes d'exploitation Apple est inférieure en France à celles d'autres systèmes d'exploitation et ce quel que soit le terminal** : elle est de 9,9 % sur postes fixes (contre 71,7 % pour Windows), 39,9 % sur tablette (59,9 % pour Android) et de 26 % sur mobile (73,6 % pour Android)⁸. Ces chiffres doivent permettre de recontextualiser l'impact de l'Apple Mail Privacy Protection (MPP) sur le marché ;
- de plus, **cette fonctionnalité n'a pas le même impact dans tous les environnements** : dans le BtoB par exemple, la lecture de courriels dans le client d'Apple représente une part encore moins moindre pour une base de données – en moyenne de 15 %. Les entreprises françaises sont en effet encore davantage qu'en BtoC utilisatrices d'environnements Windows pour les postes fixes et Android sur mobiles ;
- pour ces utilisateurs qui reçoivent des campagnes dans un client Apple, **les fournisseurs de solutions de campagnes peuvent les isoler** : Apple partage par exemple l'identifiant de son infrastructure, ce qui permet aux acteurs de traiter les informations sur ces utilisateurs en connaissant le niveau d'information ;
- dans tous les cas (BtoC comme BtoB) et au vu de la mise en place de technologies comme l'Apple MPP, le taux d'ouverture par client de messagerie tend à devoir être **mis en regard d'autres indicateurs afin de piloter une campagne**, comme le taux de clic (qui s'élève néanmoins en général à moins de 10 %). Il reste néanmoins un indicateur pertinent seul afin de suivre des évolutions dans le temps ;
- **il est possible d'isoler les utilisateurs selon le client de messagerie utilisée** : Apple partage par exemple l'identifiant de son infrastructure, ce qui permet aux acteurs d'isoler les utilisateurs en question et de le traiter en fonction de ce plus faible niveau d'information.

A noter qu'Apple n'est pas le seul acteur mettant en place des outils qui simulent des ouvertures : la messagerie de Google, Gmail, a également ce type de fonctionnement. Là aussi, la possibilité technique d'isoler les utilisateurs par client de messagerie utilisé permet aux entreprises d'utiliser des indicateurs complémentaires au taux d'ouverture pour assurer la délivrabilité et le pilotage des campagnes. Le taux d'ouverture reste également pertinent car pris en compte par les fournisseurs de messagerie comme Gmail dans leurs algorithmes pour décider de la mise en avant des courriels.

⁸ StatCounter Global Stats, « Desktop », « Tablet » et « Mobile Operating System Market Share in France – June 2025 », page consultée en juillet 2025. URL :

De manière plus globale, **il est important de rappeler que le taux d'ouverture reste un indicateur fondamental** : il permet d'avoir des données précises sur la performance d'une campagne, permettant par exemple de suivre son évolution dans le temps ou de comparer différentes campagnes. A un niveau individuel, ce sont la qualité de l'objet du courriel, le moment d'envoi et l'intérêt des utilisateurs qui peuvent ainsi être suivis, permettant ensuite d'adapter la stratégie marketing. Il permet ainsi d'ajuster le canal de communication privilégié par l'utilisateur et le volume, afin de ne solliciter les utilisateurs que s'ils ont un intérêt pour le contenu de la campagne.

Question 2 : Pourquoi la mise à disposition du taux d'ouverture est-elle un argument important pour convaincre des entreprises de choisir un outil de marketing par e-mail plutôt qu'un autre ? Quels sont d'autres critères de compétitivité alternatifs, éventuellement déterminants ?

Il s'agit d'un **indicateur parmi les plus standards dans le secteur**, que toutes les plateformes de routage permettent à leurs clients de suivre. Les offres de valeur peuvent se différencier selon la fiabilité, la granularité et la visibilité données aux clients (par campagne, par segment ou par terminal). Cela permet notamment de mettre en place des tests A/B (*A/B Testing*) ou d'adapter des automatisations, et ce en temps réel.

C'est un faisceau d'indices qui permet de prendre la décision de délivrer – ou non – un courriel donné, au cœur duquel se situe le taux d'ouverture qui permet d'améliorer performance, personnalisation et pilotage d'une campagne en temps réel. Par exemple le suivi du taux de clic est aussi important, mais il offre moins de granularité. Une même campagne peut ainsi être cliquée bien après son envoi, sans pour autant que cela soit synonyme d'un désintérêt de l'utilisateur. Le taux de conversion est également utilisé, mais l'achat pouvant être bien postérieur à la campagne, il ne permet pas non plus la même réactivité que le taux d'ouverture. Enfin, les taux de rebond ainsi que les statistiques de délivrabilité peuvent également être utilisées, mais là encore sans être aussi clé que le taux d'ouverture.

Il faut par ailleurs noter que **le courriel marketing est responsable pour les acteurs concernés d'environ 30 % de leur chiffre d'affaires**, bien davantage pour les sites d'e-commerce et de ventes privées. Il s'agit donc d'un canal indispensable pour lequel des indicateurs comme le taux d'ouverture sont clés pour personnaliser les communications et mieux cibler l'intérêt de l'utilisateur.

Question 3 : Existe-t-il des propositions alternatives d'outils de marketing par e-mail qui ont pour modèle d'affaires de proposer une solution moins intrusive ? Sinon, est-ce dû à une absence de demande, à une absence d'innovation ou à des difficultés techniques (scalabilité, intégration, compatibilité...) pour mettre en place de telles solutions ?

La demande actuellement constatée dans le secteur se porte sur des outils comme le pixel de suivi. Sa granularité est en effet particulièrement appréciée. Si la demande venait à évoluer, elle sera bien sûr étudiée par les acteurs afin de continuer à proposer des solutions adaptées aux besoins de leurs clients et prospects.

Néanmoins, il faut souligner qu'il **existe une réelle complexité technique liée à un tel changement**, en l'absence d'alternative à l'heure actuelle. Les entreprises en mesure de s'adapter à l'évolution de la demande, notamment si le cadre réglementaire se durcit, seront celles qui auront les moyens d'investir ou bien qui ne reposent pas sur l'utilisation d'un pixel de suivi pour offrir un pilotage performant à leurs clients. Il y a donc ici un **vrai risque d'une part d'effondrement des acteurs de petite taille et de taille intermédiaire**, qui n'auront pas les capacités financières nécessaires, **et d'autre part de report des budgets publicitaires vers des environnements fermés, au détriment ici d'acteurs majoritairement français et européens.**

Enfin, ce type d'évolution n'est en réalité concrètement envisageable que si les **fournisseurs de messagerie** fonctionnaient, en matière de délivrabilité, sur des règles autres que celles liées à l'activité comme c'est le cas actuellement.

Question 4 : Existe-t-il actuellement chez les fournisseurs d'outils e-mail ou à leur connaissance des projets de recherche visant à créer des innovations permettant de réduire l'intrusivité des méthodes utilisées pour mesurer les différents indicateurs ? Si oui, quels sont ces exemples d'innovations dans le domaine ?

Il n'existe pas à notre connaissance de tels projets de développement.

Question 5 : Pouvez-vous donner une estimation, quantifiée autant que possible, du gain économique (chiffre d'affaires, prospects, profitabilité...) que permet actuellement la personnalisation des emails basée sur le comportement d'ouverture d'un prospect ? Comment estimez-vous l'impact de l'introduction d'un opt in sur ce gain ? Justifiez votre réponse en explicitant les canaux de transmission et la taille des effets. L'estimation peut prendre la forme d'un intervalle si nécessaire.

Certains de nos membres nous ont partagé les éléments suivants :

- **le ciblage uniquement via le taux de clics ferait perdre en efficacité le canal** : en effet, le ratio coûts d'une campagne (temps de préparation, créa) et bénéfices retirés de celle-ci avec un ciblage possible uniquement sur un très petit nombre de personnes deviendrait négatif ;
- **pour les acteurs fournisseurs de solutions, perte de chiffre d'affaires de 70 % et rentabilité négative** : pour conserver une bonne réputation des canaux courriels et y assurer une bonne délivrabilité, il ne faut envoyer de campagnes que sur les adresses actives (c'est notamment le cas pour les utilisateurs de fournisseurs de messagerie type Gmail et Hotmail). Avec l'introduction d'un opt-in, les indicateurs d'ouvertures ne pourront plus être exploités et le ciblage ne se fera plus que sur les personnes ayant cliqué dans un lien présent dans une campagne. En comparant le volume d'ouvertures et celui de clics, on peut estimer la perte en volume envoyé et donc approximativement la perte de chiffre d'affaires. Ce calcul donne pour certains de nos membres une perte de chiffre d'affaires de 70 % et une rentabilité négative en prenant en compte les charges fixes (salaires principalement) ;

- pour les acteurs clients de ces solutions, **le volume d'affaires issu des communications CRM pourrait baisser de 10 à 15 %** : la performance commerciale globale ainsi que l'activité s'en trouveraient ainsi affectées.

Le très faible taux d'opt-in estimé, tel que décrit dans la section 2. de notre réponse, conduit plutôt certains acteurs du secteur à anticiper que la mise en place de campagnes différenciées (consenties et non-consenties) n'apporterait pas suffisamment de bénéfices. **Il est ainsi envisagé par des entreprises d'abandonner totalement cette fonctionnalité.**