

# Consentement multi-terminaux

## Consultation publique

Association PURR

27 mai 2025

Par ce présent mémoire, notre association souhaite participer à la consultation organisée par la CNIL en ce qui concerne le projet de recommandation sur le consentement multi-terminaux.

Vous trouverez donc ci-dessous notre position.

## 1 SUR LE CONTEXTE DE L'ORGANISATION DE CETTE CONSULTATION

À titre liminaire, notre association souhaite rappeler la problématique déjà soulevée devant le Conseil d'État (recours en annulation de cette concertation, affaire n° 501240, 28 janvier 2025) de l'organisation partielle de concertations privées préalablement à cette consultation publique.

Par une réponse à la demande CADA n° 20004947 du 28 avril 2025, vos services nous ont apporté des éléments supplémentaires montrant qu'un certain nombre d'entités (au moins neuf), inconnues à ce jour puisqu'anonymisées par vos services, ont déjà pu prendre connaissance de votre projet de délibération et ce dès septembre 2024.

PIÈCE 1 – Invitation à participation à une concertation privée, CNIL, 09 septembre 2025

Madame, Monsieur,

Nous nous permettons de revenir vers vous en vue de la réunion portant sur **l'élaboration d'une recommandation sur le recueil du consentement multi-terminaux en univers logué le 23 septembre 2024 de 10h30 à 12h00, dans nos locaux.**

Comme convenu, vous trouverez ci-joint le projet de recommandation rédigé par les services sous la supervision de Madame [Laurence FRANCESCHINI](#), Commissaire en charge du sujet.

Je précise qu'il s'agit d'un **projet confidentiel** qui ne peut être partagé qu'avec vos membres pour assurer une remontée des acteurs les plus concernés en amont de la réunion.

Ces entités ont déjà pu procéder à des commentaires voire à des modifications de la délibération envisagée et ont pu ainsi bénéficier d'un avantage indéniable pour intégrer leurs avis et intérêts dans le projet de délibération.

## PIÈCE 2 – Proposition de modification du projet de délibération, entité inconnue

11. Cette première condition sera en particulier satisfaite si les finalités pour lesquelles le consentement est sollicité et les responsables du traitement qui se prévalent du consentement pour leurs opérations de lecture ou d'écriture sont strictement identiques, indépendamment du terminal utilisé.

12. En deuxième lieu, le responsable du traitement doit offrir aux utilisateurs tant la possibilité d'accepter que de refuser les opérations de lecture ou d'écriture avec le même degré de simplicité. De plus, conformément à l'article 7.3 du RGPD, il doit être aussi simple de retirer son consentement que de le donner. Par conséquent, les choix formulés par l'utilisateur doivent avoir une portée identique : si le consentement peut être donné en une fois pour plusieurs terminaux, il doit en être de même pour le refus et le retrait du consentement.

13. Enfin, les utilisateurs doivent être informés de la portée du consentement avant de pouvoir exercer leurs choix afin que le consentement puisse être éclairé : l'information des personnes doit notamment préciser que les choix seront appliqués pour tous les terminaux sur lesquels l'utilisateur se connecte à son compte titulaire du compte s'authentifie.

**7.1 - Adapter l'information aux caractéristiques du consentement multi-terminaux**

14. Une attention particulière doit être portée à l'information des personnes. En effet, pour que le consentement soit éclairé, l'utilisateur doit être informé de la portée de ses choix au moment où ceux-ci sont effectués. Il doit comprendre, en particulier, la manière dont ses choix auront un impact sur le suivi de sa navigation via d'autres terminaux connectés au même compte.

15. Cette information peut se faire, par exemple, par le biais de la fenêtre de recueil du consentement (aussi appelée *consent management platform* ou CMP). La CNIL recommande que l'information relative à la portée des choix effectués et la possibilité de les modifier soit ensuite rappelée :

- au niveau de la page d'authentification du titulaire du compte ;
- à chaque connexion au compte et indépendamment du terminal avec lequel l'utilisateur se connecte, à l'aide d'un bandeau d'information qui indique, le cas échéant, si les choix associés au compte ont été enregistrés ou modifiés.

**7.2 - Gérer la contradiction entre les choix formulés au niveau du navigateur et ceux enregistrés sur le compte**

*S'agissant des solutions pour gérer la contradiction entre les choix formulés au niveau du navigateur et ceux enregistrés sur le compte*

16. Lorsque des traceurs sont utilisés dans un univers non logué, un terminal sur lequel aucun choix n'est enregistré (lors d'une première visite sur le site via le terminal ou quand les traceurs précédemment déposés sur le terminal ont été effacés) va afficher

Condition de validité importante.

Condition de validité importante.

Condition de validité importante.

Complément d'information vs précédente recommandation, important.

Nous proposons d'utiliser « authentification du titulaire du compte » qui nous semble être le sens recherché.

Attention, une connexion pourrait être entendue comme une opération qui se produit à chaque accès au service.

L'utilisation du terme « connexion » ou « Se connecter » dans les formulaires en ligne nous semble devoir être vu comme une terminologie vulgarisée et peu adaptée au présent document.

Mis en forme : Non Surlignage

Mis en forme : Non Surlignage

Mis en forme : Non Surlignage

Corrélativement au précédent commentaire : remplacer par « authentification », veiller à ce que le terme connexion, ambigu soit le moins utilisé au sein de la recommandation (proposition : remplacer par « authentification au compte » ou « accès du titulaire du compte » suivant les cas).

A voir en fonction des échanges en séance : cette information via un bandeau ultérieurement affiché peut-elle être rendue obligatoire ou doit-elle être plutôt considérée comme une bonne pratique ?

Il nous semble que les avis des agents convergeraient in fine vers la bonne pratique.

3

Nous nous retrouvons donc aujourd'hui à devoir participer à une consultation biaisée où nous devons dorénavant aujourd'hui non seulement étudier, commenter et critiquer la proposition initiale de vos services mais aussi des modifications déjà réalisées à la demande de ces tiers.

Par la même réponse à notre demande CADA, les services de la CNIL nous ont aussi indiqué que ce projet de délibération n'est pas une initiative propre de la CNIL mais une demande réalisée par des entités, *a priori* en lien avec le secteur de la publicité.

## Résumé

---

Plusieurs professionnels (du secteur de l'audiovisuel) et têtes de réseaux (notamment ■■■■■) ont exprimé leur intérêt sur la possibilité de mettre en place des dispositifs de consentement croisé pour lesquels le consentement donné vaut pour tous les terminaux avec lesquels l'utilisateur navigue sur un même site web (également appelé consentement « *cross-device* » ou multi-terminaux).

C'est pourquoi, il a été décidé d'élaborer un projet de recommandation relative au consentement multi-terminaux, qui est aujourd'hui soumis à l'adoption du Collège (annexe 1 – Projet de recommandation).

Ce projet de délibération a donc pour vocation à protéger les intérêts de Responsables de Traitement plus que ceux des Personnes Concernées et a été réalisé exclusivement en ce sens.

Il sera aussi rappelé, même au sein de ces concertations privées, d'une partialité de la CNIL, laissant plusieurs réunions étalées sur plusieurs mois aux entités commerciales pour s'exprimer alors qu'elle convoquera en urgence et sur un unique créneau les représentants des Personnes Concernées (dont l'AFCDP).

## 2 SUR LA POSSIBLE ILLÉGALITÉ DU CONSENTEMENT MULTI-TERMINAUX

Il sera rappelé que le RGPD n'autorise pas d'exception « multi-terminaux » en ce qui concerne l'expression du consentement.

De plus, dans ses lignes directrices 03/2022, le CEPD indique d'ailleurs

Cohérence entre les différents appareils : lorsque la plateforme de médias sociaux est accessible à partir de différents appareils (par exemple, ordinateur, smartphones, etc.), les informations et les paramètres relatifs à la protection des données devraient se trouver aux mêmes endroits dans les différentes versions et être accessibles par le même biais et les mêmes éléments d'interface (menu, icônes, etc.).

À la lecture de ces lignes directrices, le CEPD entend donner une certaine homogénéité et cohérence aux interfaces de consentement, ceci afin que l'utilisateur puisse anticiper facilement où et comment va se réaliser ce consentement.

Le consentement multi-terminaux remettrait ici en cause cette stabilité souhaitée par le CEPD dans le sens où, à position et interface identique, le comportement associé à l'acceptation, refus ou retrait de consentement sera différencié en fonction de critères autres non envisagés à l'époque par le CEPD (mesure de réduction de l'exposition aux bannières, modalité de gestion des conflits, etc).

Le fait d'être connecté ou non, d'être en train de se connecter ou de se déconnecter, d'avoir déjà un profil authentifié ou non, de passer d'un terminal à un autre, d'utiliser un nouveau terminal ou un ancien, seront dorénavant autant de nouveaux éléments à prendre en compte pour déterminer la stabilité des moyens d'expression du consentement.

En l'état de la recommandation de la CNIL, qui expose d'ailleurs toute la difficulté à maintenir une telle stabilité et anticipation correcte de l'effet d'une expression de consentement par la Personne Concernée, il semble ici que le consentement multi-utilisateur remette en question la stabilité et cohérence souhaitée par le CEPD et emporterait donc l'illicéité de telles modalités de consentement

Le projet de délibération conduit donc ici à tolérer un consentement qui serait probablement illicite au sens du RGPD, à tout le moins soulève la possibilité d'une invalidation de la recommandation de la CNIL une fois les autres Autorités de Contrôle et le CEPD informés de sa publication.

### 3 SUR L'OBLIGATION DE COHÉRENCE

Dans la suite du point précédent, le RGPD, par son article 63, impose de garantir l'application cohérente du RGPD au travers de l'ensemble des États Membres.

Le projet de délibération de la CNIL conduirait la CNIL à tenir une position possiblement non reconnue voire contraire à la position d'autres Autorités de Contrôle.

Ceci pourrait conduire à placer les Personnes Concernées dans des situations inextricables et à des décisions contraires entre Autorités de Contrôle.

Qu'advierait-il par exemple d'une entité espagnole offrant des services en France et souhaitant utiliser du consentement multi-terminaux toléré par la CNIL, ceci alors que l'AEPD serait Autorité de Contrôle chef de file (au sens de l'article 60 du RGPD) et pourrait alors condamner un tel consentement multi-terminaux. Ou inversement une Personne Concernée ester devant l'AEPD, ne reconnaissant pas le consentement multi-terminal, contre une entreprise française, où la CNIL reconnaît ce mode de consentement ?

Il semble ici nécessaire que la CNIL présente son projet de délibération au CEPD et aux autres Autorités de Contrôle afin d'obtenir une application cohérente du RGPD dans tous les États Membres.

Ceci d'autant plus que la Commission Européenne, dans son rapport 2024 sur l'application du RGPD, appelle à une plus grande cohérence du RGPD et à une meilleure coopération entre Autorité de Contrôle.

### 4 SUR LA COMPLEXIFICATION DU CONSENTEMENT

Au point 7(3) de son projet de délibération, la CNIL aborde la problématique posée par le consentement multi-terminaux en ce qui concerne l'apparition de contradiction entre un consentement, refus de consentement ou retrait de consentement entre l'environnement authentifié et celui non authentifié.

Dans la suite du point ?? de notre réponse, cette situation semble conduire à une illicéité d'un tel consentement, puisque le consentement doit être éclairé univoque et simple (article 6).

Une telle complexité de consentement est manifestement contraire à ces trois critères, rendant impossible pour une Personne Concernée d'anticiper correctement les effets d'une acceptation, refus ou retrait d'un consentement.

Les bannières cookies sont déjà suffisamment complexes, ne pouvant alors en aucun cas respecter le critère de simplicité et d'éclairé du RGPD (voir en cela le mémoire associé à la campagne de plaintes portée par notre association, violation n° 3 « *vice de consentement par*

*consentement non spécifique et non éclairé »).*

L'ajout d'un niveau de complexité supplémentaire avec l'introduction des informations et gestion des conflits et contradictions entre environnement authentifié et non authentifié ne fera que renforcer la violation d'un consentement valide (libre, explicite, spécifique, univoque, éclairé et positif).

En l'état du projet de recommandation, il ne nous paraît donc pas possible d'obtenir valablement un consentement licite dans un environnement multi-terminaux.

Ce projet implique en effet des systèmes d'information supplémentaires concernant les contradictions possibles entre les environnements authentifiés et non authentifiés, alors que les quantités d'information dans les CMP sont telles que les utilisateurs n'en lisent tout simplement plus le contenu.

Il serait attendu de la CNIL qu'elle mette déjà fin aux abus constatés en la matière et en rende les CMP licites vis-à-vis de l'obligation de simplicité et de compréhension imposée par le RGPD, avant d'autoriser à ajouter encore plus de niveau et de finesse d'information.

## **5 SUR LA FATIGUE À L'EXPOSITION AUX BANNIÈRES COOKIES**

Lors de la consultation privée organisée préalablement à cette consultation publique, les entités consultées se sont réfugiées derrière la fatigue à l'exposition aux bannières cookies.

PIÈCE 4 – Rapport sur la modification de la recommandation « cookies et autres traceurs » proposant des modalités pratiques de mise en conformité du consentement multi-terminaux (cross-device), CNIL, 27 mars 2025

19. Le projet de recommandation prévoit que les utilisateurs doivent être informés de la portée « *multi-terminaux* » du consentement avant de pouvoir exercer leurs choix.
20. Pour que le consentement soit éclairé, le projet de recommandation, initialement présenté lors de la concertation, prévoyait que l'information relative à la portée des choix effectués et la possibilité de les modifier soit rappelée **à chaque authentification au compte à partir d'un nouveau terminal et indépendamment du terminal avec lequel l'utilisateur se connecte.**
21. **Les professionnels ont demandé la suppression de cette recommandation,** considérant qu'elle :
  - n'aurait pas de fondement juridique ;
  - aurait des effets de bord importants (même hors consentement multi-terminaux) ;
  - pousserait au retrait du consentement donné ;
  - **participerait à la fatigue du consentement.**

Cette justification de leur part est très étonnante puisque la situation actuelle de surexposition aux bandeaux cookies est générée par les mêmes entités, au travers de bandeaux abusifs et illicites et sans mettre en œuvre aucune mesure de limitation à cette exposition.

Il sera en effet rappelé à la CNIL que la quasi-totalité des bandeaux cookies sont en pratique illicites et qu'ils correspondent plus à une solution palliative pour maintenir des traitements illicites sous couvert de respecter la législation qu'à une pratique licite et correcte vis-à-vis du RGPD.

Les bandeaux cookies correspondent à de l'extorsion de consentement afin de maintenir des traitements illicites extrêmement intrusifs (enchères publicitaires en temps réel (RTB), tracking inter-site, revente de données...) afin de maintenir des modèles commerciaux tout autant illicites et impossibles avec le RGPD.

Comme présenté aussi dans notre mémoire associé à notre campagne de plaintes (violation n° 6, « *non mitigation de la fatigue à l'exposition des bannières cookies* »), aucun Responsable de Traitement n'a jamais mis en œuvre la moindre mesure visant à limiter l'exposition aux bandeaux cookies et à la fatigue induite.

L'ancienne solution technique « Do Not Track »<sup>1</sup> n'a jamais été prise en compte, conduisant d'ailleurs à son abandon.

De même, la solution « Global Privacy Control »<sup>2</sup> aujourd'hui normalisée n'est toujours pas déployée par les CMP, alors même que certains Responsables de Traitement maîtrisent

---

1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/DNT>

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

manifestement la technologie (voir l'exemple de Sephora, condamné aux États-Unis et enjoint à l'implémenter<sup>3</sup> mais ne la déployant pas en Europe).

La proposition de recommandation va ici encore plus renforcer cette exposition intense aux bandeaux cookie, en violation des lignes directrices 05/2020 du CEPD sur le consentement :

87. Dans le contexte numérique, de nombreux services nécessitent des données à caractère personnel afin de fonctionner. Les utilisateurs reçoivent ainsi chaque jour de nombreuses demandes de consentement auxquelles elles doivent répondre par un clic ou en balayant leur écran. Cela peut mener à une certaine lassitude : lorsque trop souvent rencontré, l'effet d'avertissement des mécanismes de consentement diminue.

88. Il en résulte une situation où les informations de consentement cessent d'être lues. Cela constitue un grand risque pour les personnes concernées, dès lors que le consentement est généralement demandé pour des actions qui seraient illicites sans ce consentement. Le RGPD impose aux responsables du traitement de développer des solutions à ce problème.

En effet, les recommandations demandent à mettre en œuvre encore plus de panneaux d'information à l'utilisateur, à un point où les Responsables de Traitement eux-même en demandent à ne plus nécessiter d'interagir avec eux pour ne pas encore plus fatiguer le visiteur.

Il s'agit donc d'une recommandation qui va empirer la situation alors que la CNIL est au contraire supposée enjoindre aux Responsables de Traitement de déployer des solutions de réduction de l'exposition déjà bien trop importante aux bandeaux cookie.

La demande des entités mentionnées précédemment de supprimer toute action positive pour la fermeture de la modale d'information revient en réalité à sacrifier encore une fois la protection des droits des Personnes Concernées en échange d'une plus faible exposition aux bannières.

Une telle position est intolérable et toute mesure de limitation de cette exposition ne devrait emporter aucun effet négatif sur les droits des Personnes Concernées.

Il reviendrait ici, au mieux, aux Responsables de Traitement de trouver une solution technique pour résoudre le problème de contradiction entre les environnements authentifiés et non authentifiés qui ne remette pas en cause les droits des Personnes Concernées tout en n'exposant pas les utilisateurs à plus de bannières de consentement.

Il nous semble effectivement impossible, pour des raisons autant techniques que légales, de concilier à la fois non exposition aux bannières et non perte de droits pour les Personnes Concernées. Faute d'une telle solution, le consentement multi-terminaux doit être considéré comme illicite et donc interdit et sanctionné par la CNIL.

---

3. <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement>

## 5.1 Sur l'impossibilité technique de la synchronisation de consentement entre les environnements authentifiés et non authentifiés

Dans son projet de recommandation, la CNIL imposerait que le refus ou retrait de consentement soient synchronisés entre les terminaux.

Une fois encore, le seul retrait de consentement, tel que définit par la législation et les recommandations en vigueur, n'est aujourd'hui mis en œuvre par aucun Responsable de Traitement (voir en cela la décision SAN-2024-019 à l'encontre d'Orange ou notre mémoire concernant la campagne de plaintes cookie).

Techniquement, il est très difficile sinon impossible de déjà garantir l'effectivité d'un refus et pire, d'un retrait de consentement sur un unique environnement et terminal.

L'ajout d'une grande complexité supplémentaire pour espérer la propagation du refus ou retrait de consentement à un autre terminal, est en réalité d'une difficulté technique ou générant des niveaux d'incohérences d'un niveau substantiellement plus élevé que ce qui n'arrive déjà pas à être traité correctement par les Responsables de Traitement.

Une fois encore, nous souhaiterions que la CNIL obtienne d'abord la mise en conformité des Responsables de Traitement en ce qui concerne le refus et retrait de consentement en environnement mono-terminal avant de leurs autoriser la mise en œuvre en environnement multi-terminaux.

## 5.2 Sur la prise en compte d'éléments extérieur d'expression de consentement

Le projet de recommandation n'aborde aucunement la problématique de l'incohérence de l'état du consentement au travers de l'expression d'un consentement par des mécanismes extérieurs aux Responsables de Traitement, par exemple les mécanismes de diminution de la fatigue aux bandeaux cookies comme DNT ou GPC.

La recommandation se résume en effet à étudier les incohérences exclusivement à la main des Responsables de Traitement. L'introduction de mécanisme comme GPC présenté précédemment ajoute des combinaisons exponentielles d'incohérences possibles.

Quid par exemple de l'acceptation d'un consentement sur un terminal authentifié n'ayant pas GPC actif puis la consultation du même contenu au travers d'un terminal authentifié avec GPC actif? Une telle configuration devrait-elle être l'expression d'un retrait de consentement et conduire à l'invalidation du consentement dans l'environnement authentifié?

De même, l'activation *a posteriori* de GPC sur le terminal authentifié initial doit-elle conduire au retrait de consentement dans l'environnement authentifié?

Il devient matériellement impossible pour le Responsable de Traitement d'implémenter de manière compréhensible et reproductible une logique tenant compte d'autant de paramètres

que pour la Personne Concernée de pouvoir comprendre et anticiper l'état de son consentement dans un tel environnement.

Cette problématique des expressions de refus/rejet de consentement par des outils tiers rend impossible une compatibilité des recommandations de la CNIL avec les critères de simplicité et de compréhension imposés par le RGPD en ce qui concerne le consentement.

### **5.3 Sur les bandeaux non interactifs d'information concernant les incohérences de consentement**

Dans sa recommandation, et à la demande des Responsables de Traitement, la CNIL propose de ne pas imposer d'interaction avec les bannières d'information suite à une incohérence de consentement entre terminaux.

Une telle proposition nous semble illicite et revient à la problématique pré-RGPD de l'illicéité d'un consentement exprimé de manière non positive.

Cette bannière d'information concerne ici bel et bien une information majeure et importante concernant un consentement. Il ne s'agit donc pas d'un bandeau annexe mais d'une partie pleine et entière relative à l'expression de consentement.

Il ne peut donc en être autrement que d'imposer aux Responsables de Traitement une interactivité obligatoire sur cette bannière, ceci afin de respecter l'obligation d'acte positif concernant l'expression de consentement (article 7).

Si les Responsables de Traitements considèrent que cette solution expose trop leurs utilisateurs à des bannières cookies, il leur reviendra, comme imposé par les lignes directrices du CEPD, de trouver des moyens de limiter cette fatigue, par exemple en ne mettant tout simplement pas en œuvre un consentement multi-terminaux.

### **5.4 Sur l'interdiction de conception trompeuse**

À son point 7.1, la CNIL indique que la mise en œuvre de sa recommandation ne pourra être mise en œuvre que dans les conditions juridiques rappelées dans les lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978.

Le projet de recommandation actuel se limite à citer les paragraphes 2-1 et 2-3 de l'article 2 de ces lignes directrices.

Nous souhaiterions y voir indiqué explicitement aussi le paragraphe 2-4 en ce qui concerne l'interdiction de recours à des pratiques de conception trompeuse visant à extorquer le consentement des utilisateurs.

Ici aussi, il serait attendu de la CNIL d'imposer d'abord aux Responsables de Traitement de se mettre en conformité sur les bannières mono-terminaux déjà existantes avant d'autoriser

du consentement multi-terminal.

Le refus de consentement, faisant aujourd'hui massivement l'objet de conception trompeuse ayant pour finalité d'extorquer un consentement à l'utilisateur (voir en cela notre mémoire concernant notre campagne de plaintes cookies, violation n°2 « *vice de consentement par extorsion de consentement* »), aura des effets encore plus délétères en environnement multi-terminaux.

En environnement multi-terminaux, une conception trompeuse contraignant l'utilisateur à une acceptation du consentement, bien souvent sans même lire la bannière (problème de la fatigue liée à l'exposition aux bannières), aura des conséquences bien plus violentes, avec une propagation de ce consentement extorqué à l'ensemble des terminaux de l'utilisateur.

## 5.5 Sur l'information du consentement multi-terminaux

Le projet de recommandations ne précise pas à son point 7(2) l'emplacement exact de l'information délivrée à l'utilisateur.

Il serait pertinent d'imposer une information dès le premier niveau de la bannière cookie, ceci afin de bien informer y compris les utilisateurs n'allant pas consulter les autres niveaux et accepter ou refuser les cookies.

Il serait aussi souhaitable dans cette recommandation d'imposer une information concernant l'ensemble des finalités qui seront transférées aux autres terminaux (publicité ciblée, statistiques d'audience. . .) et non une formulation vague exprimant uniquement la synchronisation à venir.

## 5.6 Sur la politique de résolution des incohérences

Le projet de recommandation propose deux possibilités de résolution des incohérences, la modalité 1 privilégiant les choix du nouveau terminal non authentifié à ceux du compte authentifié, et la modalité 2 privilégiant l'inverse.

Nous souhaiterions que la CNIL ne retienne qu'une seule modalité, ceci pour éviter tout problème d'incompréhension des utilisateurs qui seraient possiblement exposés aux deux modalités, faute de solution unique retenue par les Responsables de Traitement, celle-ci n'étant que souhaitée et non imposée par la CNIL.

Nous souhaiterions privilégier uniquement la seconde modalité, ceci afin d'éviter à un utilisateur consentant à de nouvelles finalités en environnement non authentifié de risquer de ne pas anticiper qu'elles seront aussi dorénavant actives sur l'ensemble de ses terminaux.

## 5.7 Sur la non transmission de données à caractère personnel aux CMP

Nous trouvons insuffisantes les protections considérées par la CNIL en ce qui concerne le recoupement possible entre un environnement authentifié et un non authentifié.

Le projet de recommandation fait état de l'interdiction de transmission de données à caractère personnel (DCP) aux CMP, mais ce point nous interroge.

Une fois encore, l'état actuel des bannières cookies comportent manifestement des DCP alors que les Responsables de Traitement le réfutent. Voir en cela la saga IAB/TCF avec déjà plusieurs condamnations et reconnaissance du TCF comme DCP y compris par la CJUE alors que l'IAB et les Responsables de Traitement persistent depuis bientôt 10 ans à maintenir ces échanges de DCP sous couvert qu'elles n'en seraient pas.

De plus, il sera rappelé le très grand danger lié aux recoupements d'informations n'apparaissant pas comme des DCP mais générant pourtant *de facto* des DCP. Nous renvoyons par exemple aux travaux du LINC sur ce sujet et ce dès 2016<sup>4</sup> ou encore ses travaux de désanonymisation de données supposées anonymes<sup>5</sup>.

En l'état, l'absence de transmission de DCP au CMP, à supposer qu'elle soit en elle-même déjà effective, ne suffit donc pas à protéger les utilisateurs d'un risque d'identification.

Nous souhaiterions une position plus forte sur ce sujet.

Les données non DCP en tant que telles, à supposer qu'il soit même possible qu'il en existe, ne sont pas couvertes *stricto sensu* par le RGPD mais l'esprit de la loi et l'article 5 du RGPD imposant la minimisation des données pourrait être une piste de renforcement.

Il serait ainsi souhaitable de ne procéder au transfert que des seules informations peu risquées en termes d'identification et sans effet notable sur les droits des Personnes Concernées (par exemple l'autorisation de statistiques d'audience ou l'acceptation de participation à l'amélioration des services) et non à celles risquées en terme de désanonymisation ou à risques importants sur les droits (publicité ciblée, RTB...).

## 5.8 Conclusions

Notre association s'oppose donc vertement à cette proposition de recommandation de la CNIL.

Sur la forme, les conditions d'organisation très partiales interrogent sur la neutralité de la CNIL et au pire remettant en cause la garantie d'un niveau élevé de protection des droits des Personnes Concernées (considérants 10 et 11 du RGPD, et arrêt joint C-26/22 et C-64/22 de

---

4. <https://linc.cnil.fr/nouvelles-frontieres-des-donnees-personnelles>

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

la CJUE), la forme et le contexte de cette délibération est en soit dangereux.

Il sera rappelé que notre association a réalisé un recours devant le Conseil d'État demandant purement et simplement l'annulation de l'organisation de ces concertations.

Au fond, la recommandation proposée viole le RGPD sur plusieurs points.

De par l'esprit-même de cette législation, un tel consentement multi-terminaux n'est pas autorisé par le RGPD. Même à supposer qu'une interdiction explicite n'est pas présente, les modalités pratiques de mise-en-œuvre contreviennent aux obligations liées au consentement (caractère éclairé, spécifique, univoque, positif et simple).

Les problèmes soulevés lors des concertations privées indiquent bien une difficile légalité de tels traitement et la CNIL cherche uniquement par tous les moyens à maintenir les modèles commerciaux illicites des Responsables de Traitement *via* des recommandations *ad-hoc*, d'ailleurs rédigées à leur demande.

La recommandation actuelle sur le consentement multi-terminaux augmente le défaut d'information des Personnes Concernées, complexifie encore plus les CMP, rend encore plus incompréhensibles les effets d'un consentement. Elle rend ici donc encore plus illicite les consentements déjà extorqués au travers des CMP existants.

Les problématiques de contradiction entre environnement authentifié et non authentifié vont aussi soit augmenter la fatigue à l'exposition aux bannières, soit rogner encore plus sur les droits des Personnes Concernées déjà bien mis à mal avec les CMP existantes.

**Nous ne pouvons donc que demander à la CNIL d'abandonner totalement ce projet de délibération et de rejeter la demande initiale des entités non identifiées de légaliser ce consentement multi-terminaux.**

**Nous demandons au contraire à la CNIL de mettre d'abord fin aux exactions des Responsables de Traitement en ce qui concerne leur non-respect du RGPD *via* l'usage de CMP illicite, et uniquement ensuite d'envisager à nouveau du consentement multi-terminaux dans un éco-système sain.**

Nous sommes persuadés qu'avec des CMP licites et la disparition d'une bonne partie des traitements illicites masqués derrière elles, la question du multi-terminaux ne se posera même plus.

Dans le cas où la CNIL maintiendrait de telles recommandations, nous souhaiterions la mise en conformité préalable des bandeaux cookies déjà existants en environnement mono-terminal avant tout déploiement de solutions encore plus complexes et difficiles à en maîtriser la conformité.

Le projet de recommandations étant actuellement très favorable aux intérêts des Responsables de Traitement et au contraire très peu protecteur des droits des Personnes Concernées, nous souhaiterions un renforcement substantiel des garanties en la matière ceci afin de ne pas affaiblir encore plus des utilisateurs déjà très malmenés par les bandeaux actuels.

Pour l'association PURR

