Réponse à concertation
Preuve de recueil du consentement

Association PURR

6 mars 2026

L'association Pour un RGPD respecté (PURR) défend et promeut le droit à la vie privée, le droit à la protection des données à caractère personnel (DCP), et un niveau élevé de protection des DCP.

Elle représente les Personnes Concernées (article 4(1) du Règlement général sur la protection des DCP, dit RGPD) et les Délégués à la Protection des DCP (dits DPO, article 37 et suivants du RGPD).

Par le présent mémoire, PURR entend participer à la concertation de la CNIL sur son projet de recommandation relative aux moyens de prouver le recueil de consentement dans le secteur marketing.

Table des matières

1. Sur l'organisation de cette concertation

À titre liminaire, notre Association conteste à nouveau les modalités d'organisation de cette concertation.

Comme déjà remonté à vos services le 22 janvier dernier[1], même si nous sommes très heureux d'y être conviés cette fois-ci, nous considérons comme anormal, injuste, et dangereux que la CNIL organise des concertations selon son entière discrétion, sur des sujets tenant manifestement à permettre la légalisation, par la CNIL, de pratiques massivement illicites, parfois même explicitement reconnues comme telles par les Responsables de Traitement, qui savent pertinemment ne pas pouvoir respecter la législation et demandent alors des recommandations bienveillantes à votre Commission.

En l'absence de dispositions spécifiques dans l'article 8(I)2(b) de la LIL, cette concertation relève de l'article L131-1 du Code des relations entre le public et l'administration, et de jurisprudence constante du Conseil d'État, elle devrait, à ce titre, faire l'objet d'une communication publique préalable, y compris des modalités de participation, permettant ainsi une participation de toutes les entités concernées, et non une réduction arbitraire des participants par la CNIL.

Le même article L131-1 CRPA dispose que l'administration « *assure un délai raisonnable pour participer* ». En l'espèce, le délai fixé initialement, 2 semaines et 2 jours, en pleine reprise du mois de janvier, est extrêmement bref. Un tel délai, déraisonnable, est très difficilement tenable pour une association comme la nôtre composée exclusivement de bénévoles, et il est de nature à les dissuader de participer. Une autre association de la société civile, pourtant d'envergure, a décliné votre invitation au regard du délai et de sa charge de travail. D'évidence, un tel délai n'octroie donc pas, à l'ensemble des parties-prenantes, une équitable opportunité de participation. **Nous attirons vivement la vigilance de la CNIL sur ce point**.

2. Sur l'introduction (§1)

La CNIL devrait référencer les lignes directrices 5/2020 du CEPD afin de rappeler leur existence aux Responsables de traitement et d'inscrire sa recommandation dans un corpus doctrinal existant immédiatement identifiable.

[1] CNIL-229957-1769112460

3. Sur le périmètre (§2)

La CNIL devrait expliciter, dès le début du document, qu'il porte indifféremment sur consentement recueilli aux titres des articles 6(1)a, 9(2)a, ou 49(1)a du RGPD.

Nous ne partageons pas la délimitation au seul secteur du marketing qui ne nous apparaît pas posséder de spécificités en matière de preuve de consentement. De plus, la fin de cette section laisse déjà la place à des aménagements sectoriels. Dès lors, **le projet de recommandation devrait être généralisé**, d'une part pour avoir un effet significatif, et d'autre part, pour éviter de futurs autres travaux fastidieux pour la CNIL et la société civile dont, de surcroît, la CNIL prendrait prétexte pour octroyer, aux Responsable de traitement, un nouveau délai de mise en conformité.

4. Sur le cas général (§3.1)

Notre Association ne trouve rien de fondamental à redire sur cette section, qui correspond en tout point aux obligations légales faites en ce qui concerne le recueil du consentement.

Les informations collectées permettent d'assurer la traçabilité du consentement et sa vérification a posteriori lors d'un contrôle ou d'une contestation du consentement par la Personne Concernée.

« *Le moment où elle a consenti* » pourrait contenir un exemple plus précis « *d'enregistrement en ligne* » : le journal (log) de l'applicatif qui reçoit et traite le formulaire web.

La CNIL devrait préciser que les éléments de preuve collectés en ligne devraient être signés cryptographiquement afin d'en garantir l'authenticité. De même, la CNIL devrait préciser que les documents écrits devraient, d'évidence, être signés. Or collecte pour un tiers, l'usage de ce type de données étant très limité (exclusivement en cas de contestation), l'ensemble des éléments de preuves, quel que soit le moyen de collecte, devraient être conservés en accès restreint, voire immédiatement en base archive, pour les seules finalités probatoires et de conformité. En ce sens, voir votre délibération 2021-122 portant adoption d'une recommandation sur la journalisation, points 7 et 12.

La CNIL devrait préciser que l'enregistrement d'un appel téléphonique devrait également contenir les informations délivrées à la Personne concernée. Cela permettra, en cas

de contestation, de vérifier les caractères éclairé, explicite, libre, etc. du consentement, notamment lors du démarchage de seniors. Le script d'appel n'établit pas l'information *réellement* délivrée.

Enfin, la CNIL devrait préciser les éléments supplémentaires qu'un Responsable de traitement devrait conserver pour établir, le cas échéant, que le consentement a été donné ou autorisé par le titulaire de l'autorité parentale au titre de l'article 8(2) du RGPD.

5. Sur l'environnement non authentifié (§3.2)

La CNIL devrait préciser et illustrer les « *éléments relatifs au contexte de la navigation* » : il s'agit d'éléments *déjà* connus du Responsable de traitement au moment de l'expression du consentement, comme l'adresse IP du terminal, son User-Agent (marque, modèle et version du système et du navigateur web), etc.

Le projet de recommandation est insuffisant en ce qu'il ne permet pas de s'assurer de la licéité du consentement.

Il a été déjà porté à notre connaissance que des Responsables de Traitement usurpent la double validation (double opt-in) en insérant des données générées comme « preuve » du consentement.

Les services instruction et contrôle de la CNIL ont même, à de nombreuses reprises, échoué à identifier de tels consentements extorqués, avec des dates de validation du consentement antérieures à l'envoi du courriel de confirmation (Infogreffe, plainte n° 44-11689), ou avec des données soumises via des adresses IP ne pouvant matériellement pas appartenir à la Personne Concernée (Bouygues Telecom/Reworld/Max de Deal, plainte n° 44-47920 ou BUT/LiveData Solutions/Wonderlead, plainte n° 44-134719).

Il en est suspecté de même sur des jeux concours fictifs, les services de la CNIL étant probablement passés à côté de cette usurpation lors de la sanction des entités Tagada Media, Solocal et Caloga (plaintes n^{os} 44-100007 et 44-88053).

En l'état, la proposition actuelle de la CNIL permet trop facilement une usurpation du consentement. Elle se limite en effet quasi exclusivement à imposer la collecte des

éléments probants *en amont* de la double validation, et non *au moment* de cette double validation.

Notre Association propose ainsi de **renforcer la preuve de consentement obtenue par la confirmation au travers du second canal** (courriel, téléphone…) en appliquant alors, à nouveau, les exigences de la section 3.1 une fois que la Personne Concernée est identifiée via ce second canal.

Ceci permet de collecter les mêmes éléments probants (contenu exact du consentement exprimé, user-agent, cookie, IP…), mais renforcés par la double validation, et de conserver ainsi une preuve forte de l'authenticité de ce consentement et de la double validation.

Nous attirons aussi l'attention de la CNIL sur la problématique que nous avons déjà soulevée lors de notre réponse à la consultation de la CNIL sur les pixels traçants.

Les contenus traçants sont aujourd'hui très régulièrement consultés automatiquement par, entre autres, des antivirus, des fournisseurs de courriel, ou des bloqueurs de traceurs.

Il est donc nécessaire de mettre beaucoup plus en évidence **la nécessité d'une confirmation de la double validation qui soit réellement active** de la part de la Personne Concernée, et que le seul clic sur un lien ne constitue ainsi pas une preuve de consentement.

En effet, une visite simple de la page web derrière le lien de confirmation peut être une action automatisée et ne constitue donc pas nécessairement une validation explicite par la Personne Concernée. Une action explicite de la Personne Concernée reste nécessaire.

Par exemple un lien de confirmation peut rediriger vers une page web rappelant le contexte de consentement et présenter un bouton « Consentir ». Seul le clic sur ce bouton valide le consentement, et non la seule visite de la page web.

Notre Association considère aussi que, dans un environnement non authentifié, le consentement ne peut être considéré comme valide qu'après la double validation, y

compris et surtout lorsque le moyen de contact a été décliné en présentiel dans un contexte non-authentifié.

En l'état de la recommandation, cette double validation n'est présentée que comme possiblement informative (« *a minima afin de l'informer du consentement* »).

Or, la législation impose, à l'article 4(11) du RGPD, d'avoir un consentement *positif* de la part de la Personne Concernée. Sans cette double validation, le Responsable de Traitement ne peut avoir aucune assurance concernant ce critère d'action positive, et il ne peut donc pas considérer le consentement comme valide. Il ne peut donc pas commencer les traitements de données associées aux finalités en question.

Nous proposons donc de **rendre obligatoire cette double vérification**, et non pas simplement facultative comme actuellement rédigé.

En l'état actuel de la rédaction, l'exemple encadré de la page 6 est incohérent avec ce qui le précède en ce qu'il ne recommande pas de conserver l'ensemble des éléments propres à un consentement en univers non-authentifié (copies des données saisies, éléments de contexte, etc.). Or, la double validation est un moyen supplémentaire de s'assurer du consentement qui ne saurait se substituer à la collecte, même temporaire, et à la communication, à la Personne Concernée des autres éléments identifiés précédemment, notamment car ces derniers permettent à une Personne Concernée d'attester qu'elle n'a pas donné son consentement (ex. : adresse IP improbable).

Enfin, la CNIL devrait préciser que si un Responsable de traitement recourt à la double validation, il devra mettre en place un mécanisme évitant tant l'envoi d'un courriel ou d'un SMS de confirmation à un grand nombre de moyens de contact en peu de temps (par une preuve de travail, un captcha, etc.), que l'envoi, répété d'un nombre élevé de sollicitations à un même moyen de contact. De tels mécanismes concourent à **ne pas harceler des personnes par l'intermédiaire de formulaires web**. Certains de nos membres ont déjà été victimes de tels détournements de validation de consentement par des personnes malveillantes et se sont retrouvés spammés de centaines de demandes de double validation.

6. Sur l'exception pour les cookies (§3.3)

Notre Association **s'oppose vivement et totalement à l'exception concernant les cookies**.

En premier lieu, **cette exception ne trouve pas à s'appliquer en environnement authentifié** puisque, par définition, l'utilisateur y est identifié, y compris de manière pérenne. Dès lors, l'exception est dénuée, dans les faits, de sa justification. Ainsi, en cas de maintien de cette exception cookies, la CNIL doit préciser qu'elle ne s'applique pas aux cookies déposés et/ou lus en environnement authentifié.

En deuxième lieu, **le RGPD, auquel renvoie la directive e-Privacy via son article 2, ne prévoit aucune exception** à l'exigence d'une démonstration du consentement.

Il en va de même du CEPD qui, dans ses lignes directrices 5/2020, que la CNIL présente comme une « source d'inspiration »[2], en sus de rappeler cette exigence (points 104 à 107), consigne que, dans un « *environnement en ligne* », « *il ne serait pas suffisant de simplement se référer à une configuration adéquate du site internet* » (point 108), ce qu'est une preuve de procédé.

L'exception litigieuse est, en Europe, une position solitaire de la CNIL. Ce faisant, elle contribue à une fragmentation de l'application des droits à la vie privée et à la protection des données à caractère personnel, ce que le RGPD a pour objectif d'éviter (cf. ses considérants 9 et 10). En tout état de cause, elle ne contribue pas au « niveau élevé de protection des personnes physiques » recherché par le RGPD (idem).

En troisième lieu, **cette exception vide le principe de sa substance**. En effet, le consentement aux cookies et autres traceurs (ci-après, cookies) est, en volume, l'expression la moins souvent à l'initiative d'une Personne concernée, la plus fréquente, la plus courante, et aussi, généralement, la plus intrusive voire abusive, du consentement. Dès lors, une exception pour les cookies revient à dispenser de preuve le recueil le plus fréquent, fragile, et litigieux du consentement. L'exception devient alors tacitement la norme et elle vide de sa substance le principe d'une démonstration du consentement.

[2] Délibération SAN-2025-005, point 137 ; délibération SAN-2025-010, point 40

Or, une disposition de droit souple ne saurait vider de sa substance une norme juridique de rang supérieur, ni contrevenir à un principe, ni créer une situation contraire à l'intention du législateur, ni, enfin, fixer une règle nouvelle en l'absence de compétence de l'administration (CE 452668, pt. 7 ; CE 418142, pt. 2). De plus, les exceptions sont d'interprétation stricte (CE 358183, pt. 3). Il en va de même des dispositions limitant les droits octroyés par un instrument juridique de l'UE, comme le RGPD (C-311/18, pt. 84).

En l'espèce, le législateur de l'UE n'a prévu aucune exception à la démonstration du consentement, ni aucune possibilité d'en établir une. Il apparaît douteux, sur le plan légal, que la CNIL disposerait de la compétence pour y procéder, notamment via du droit souple. L'exception a pour effet de rétrécir le sens et la portée, au point, comme il a déjà été dit, de la vider de sa substance, de la preuve de consentement, qui est un droit otroyé par le RGPD visant à protéger les Personnes concernées d'un traitement faussement ou prétendument fondé sur leur consentement. Comme nous allons le voir, cette exception annihile les droits octroyés aux Personnes concernées par le RGPD. Dès lors, cette exception nous apparaît illicite.

En quatrième lieu, **l'exception pour les cookies et autres traceurs est contradictoire avec d'autres exigences du RGPD *rappelées par la CNIL***. En effet, dans ses décisions récentes concernant les cookies, la CNIL a rappelé la nécessaire effectivité du retrait du consentement en matière de cookies, y compris à l'égard des « cookies tiers ».

Ainsi, au point 147 de sa délibération SAN-2025-005, la CNIL écrit : « *Ainsi, même si la société n'avait pas la possibilité d'assurer elle-même la suppression des cookies tiers, il lui appartenait de mettre en œuvre les mesures nécessaires afin […] de porter à la connaissance de ses partenaires le fait qu'une fois son consentement retiré par l'utilisateur, les cookies qu'ils avaient déposés […] devaient être retirés.* ».

Cette position a été réitérée dans les récentes mises en demeure dans le cadre de « nos » réclamations 44-94273, 44-94282, 44-94288, 44-94290, 44-94292, 44-94293, 44-94295, 44-94296, 44-94377, 44-94378, 44-94381, 44-94383, 44-94284, 44-94385, et 44-96031 : « *il appartient* » à un Responsable de traitement « *d'effectuer les vérifications nécessaires*

et de prendre les mesures adéquates auprès de ses partenaires pour faire cesser le manquement ».

Comme l'a relevé la CNIL, le blocage, par l'éditeur du site web collecteur du consentement, des requêtes web à destination d'un Responsable de traitement tiers à qui le consentement a été transmis ne suffit pas puisque ce tiers continuera à suivre l'activité de la personne qui a retiré son consentement sur son propre site web et/ou sur les autres sites web qui déclenchent des requêtes vers lui.

Les actions de « *prendre les mesures adéquates auprès de ses partenaires* » et de « *porter à la connaissance de ses partenaires* » un retrait de consentement en vue d'« *assurer* » un retrait des cookies nécessitent forcément d'identifier les cookies en question, donc le terminal, donc l'utilisateur. Donc, un Responsable de traitement à même de rendre effectif un retrait de consentement est une entité qui dispose déjà des éléments de preuve du consentement (identifiant unique d'un cookie, adresse IP, etc). Dans le cas contraire, nous aurions en réalité une entité dans l'incapacité de répondre par exemple à des demandes d'accès ou de respecter un retrait de consentement, ce qui est une situation illégale.

Il est manifeste qu'ici les Responsables de Traitement confondent volontairement la notion d'authentification avec celle d'identification, en considérant implicitement devoir authentifier formellement la Personne Concernée. Or la seule individualisation suffit à caractériser une donnée à caractère personnel, ce que permet, par conception et finalité même, un cookie.

Les Responsables de Traitement conduisent d'ailleurs bien en pratique à une identification de la Personne Concernée sur la seule et unique base du cookie considéré, puisqu'il s'agit de la finalité même des traitements réalisés (ciblage publicitaire, reciblage…).

À l'inverse, **si la CNIL exempte de preuve du consentement, alors elle avalise également, par suite logique, l'annihilation des autres droits RGPD** (accès, opposition, limitation, effacement, etc) en matière de cookies contenant des DCP ou liés à des traitements de DCP, droits qui pourraient être exercés par tout moyen en présentant, au Responsable de Traitement, le contenu des cookies et/ou d'autres données contextuelles (adresse IP, etc). L'admission de la thèse selon laquelle il n'est pas possible d'identifier un terminal sur lequel a été déposé un cookie précis, et donc une personne physique, conduit inévitablement à cette conclusion.

Or, un traitement de données à caractère personnel est indissociable des droits d'une Personne concernée à l'égard dudit traitement. Il ne peut y avoir ni consentement ni traitement sans droits. Si les droits ne peuvent être garantis, alors le traitement *ne doit pas* être mis en œuvre. Aucune exception n'a de sens dans un tel cas sans vider encore une fois de sa substance les principes fondamentaux du RGPD. Or, une exception à un principe général qui vise à faciliter l'exercice de libertés fondamentales garanties par le droit primaire de l'UE est d'interprétation stricte (C-476/01, pt. 72), notamment quand elle constitue un obstacle à la réalisation d'objectifs fondamentaux d'un règlement de l'UE (C-90/22, pt. 62).

En cinquième lieu, **l'hypothèse qui fonde cette exception**, à savoir que l'utilisateur ne serait pas identifié et que son identification, dans le cadre de la démonstration du consentement, rendrait le consentement plus intrusif que nécessaire, **est factuellement inexacte**. Au demeurant, la CNIL l'affirme sans la démontrer ni l'étayer, alors que la charge de la preuve des conditions requises par une exception lui incombe (C-900/19, pt. 29). Ce faisant, la CNIL ne saurait se prévaloir de la circonstance que son exception viserait à garantir un plus grand respect des droits à la vie privée et à la protection des données à caractère personnel, notamment le principe de minimisation, et, qu'à ce titre, son interprétation devrait aussi sauvegarder son effet utile et respecter sa finalité (en ce sens, C-516/17, pts. 54-55).

D'abord, il sera rappelé qu'il n'y a aucun besoin d'identifier nommément une personne physique, et que, comme indiqué précédemment, le cookie lui-même est en réalité le vecteur d'identification. Au point 3.2 du projet de recommandation, la CNIL présente les cookies comme des « *informations de contexte dont dispose déjà le responsable de traitement* » dans un « *environnement non authentifié* ». La CNIL reconnaît ainsi qu'ils peuvent permettre d'identifier une personne physique, notamment pour lui permettre d'exercer ses droits, grâce aux identifiants techniques uniques qu'ils contiennent ou constituent.

Une telle reconnaissance est également consignée dans la récente recommandation sur le consentement multi-terminaux[3], notamment à son article 7.5, par la communication

[3] https://www.cnil.fr/fr/cookies-et-autres-traceurs-recommandations-finales-sur-le-consentement-multi-terminaux

éventuelle, à une Consent Management Plateform (CMP), d'un identifiant technique rattaché à un utilisateur, et, à l'article 7.4, par la distinction entre environnement authentifié / non authentifié et entre les différents utilisateurs d'un même terminal.

Ensuite, il sera rappelé qu'à l'article 5(3) de la directive e-privacy, les cookies soumis au consentement sont ceux qui ne sont pas strictement nécessaires, ni pour effectuer une transmission électronique, ni pour fournir un service expressément demandé par l'utilisateur. Ces cookies, et les **traitements sous-jacents de données à caractère personnel, sont parmi les plus intrusifs et les plus individualisés** : suivi / profilage, publicité ciblée, plafonnement publicitaire (capping[4]), reciblage publicitaire, calcul du taux de conversion, etc. Ces traitements perdurent durant de nombreux mois (13 maximum). Ainsi, le prétendu caractère intrusif de la preuve du consentement s'efface derrière celui, avéré, de la finalité pour laquelle il a été recueilli, et l'individualisation peut être mise au service d'une démonstration du consentement.

À titre d'exemple, avec des éléments à disposition des éditeurs de sites web et de leur CMP, comme les cookies, l'adresse IP, etc, la TC String du Transparency and Consent Framework (TCF) de l'IAB identifie suffisamment précisément un utilisateur afin de faciliter la vente de publicité ciblée[5].

Autre exemple : les CMP ou assimilées mettent en œuvre de la métrologie des bandeaux cookies, c'est-à-dire de la mesure des interactions des utilisateurs avec ceux-ci. Voir, par exemple, la CMP Axeptio[6], le produit Gimii[7], ou la réponse de l'Alliance Digitale à la consultation publique de la CNIL sur les pixels de suivi[8]. Ces mesures sont d'abord individuelles avant d'être agrégées, et, pour qu'elles soient pertinentes, des traitements individualisants sont mis en œuvre, comme le dédoublement, l'isolement heuristique des dysfonctionnements techniques, etc.

Enfin, il découle de ce qui vient d'être exposé, que les éditeurs de sites web qui déposent des cookies disposent déjà des éléments nécessaires à une preuve du consentement listés aux sections 3.1 et 3.2 : l'identifiant technique figurant dans le cookie (ce que

4. Délibération CNIl SAN-2025-005, points 73 et 84 ; délibération CNIL SAN-2022-027, point 55
5. Arrêt C-604/22 de la CJUE, notamment son point 29
6. https://www.axept.io/fr/cookie-banner, voir « *Vos analytics de consentement* »
7. https://gimii.fr/faq/, voir « *Gimii respecte-t-il le RGPD (Règlement Général sur la Protection des Données) ? Est-ce validé par la CNIL (Commission nationale de l'informatique et des libertés) ?* »
8. https://www.alliancedigitale.org/publication/projet-de-recommandation-relative-aux-pixels-de-suivi-dans-les-courriers-electroniques/, note 6 page 9 sur le taux de consentement aux cookies

la CNIL nomme « *un identifiant de session* » dans la section 3.1), et/ou l'horodatage, et/ou le journal de la CMP et des interactions dont elle a fait l'objet, et/ou les données soumises (ex. : la TC String), et/ou des informations de contexte (adresse IP, User-Agent, etc.). Ainsi, contrairement à ce qu'affirme la CNIL, l'obtention de la preuve d'un consentement aux cookies ne nécessite pas de rendre le traitement plus intrusif qu'il ne l'est.

En dernier lieu, la « preuve de procédé » s'est montrée insuffisante et inefficace pour garantir un recueil licite du consentement[9]. Il est grand temps de rehausser le niveau d'exigence et de permettre un réel et effectif exercice des droits RGPD, et non rendre encore plus difficile l'exercice de ceux-ci.

Nous nous retrouvons à nouveau dans une situation où les Responsables de Traitement ont mis en œuvre des traitements massivement illicites et où la CNIL se retrouve à leur ménager des portes de sortie permettant leur maintien à tout prix.

L'écosystème mis en place par les Responsables de Traitement en ce qui concerne les cookies est connu de très longue date pour violer la législation en vigueur sur quasiment l'ensemble du texte.

Il revient aux Responsables de Traitement de trouver des solutions techniques à leurs problèmes auto-construits ou, le cas échéant, à supprimer purement et simplement leurs traitements.

Il ne revient pas à la CNIL de les protéger en leur aménageant des exceptions ad hoc pour légaliser de tels traitements, mais au contraire il serait attendu de la CNIL l'adoption des sanctions et/ou des mesures correctrices qui s'imposent.

Il est rappelé que notre Association porte actuellement plus de quarante plaintes contre les bannières cookies, et que l'intégralité du marché contrevient à la réglementation sur plus d'une dizaine de points[10]. La CNIL a d'ailleurs reconnu le problème, en sanctionnant par une mise-en-demeure la totalité de la vingtaine de réclamations déjà traitées à ce jour, le restant allant certainement relever des mêmes sanctions.

---

9. Voir https://noyb.eu/en/noyb-win-conde-nast-fined-eu750000-placing-cookies-without-consent et https://noyb.eu/en/say-no-cookies-yet-see-your-privacy-crumble

10. Campagne de plaintes « modalités cookies »

Dans son principe, la notion de « preuve de procédé », d'autant plus dans le contexte des cookies, annihile totalement toute possibilité de consentement positif.

En effet, la Personne Concernée ne dispose, la plupart du temps, d'aucun moyen d'identifier, encore moins dans le temps et sur ses multiples terminaux, les cookies consentis ou non et de pouvoir contester avoir donné son consentement à tel ou tel traitement, ou plus simplement de pouvoir retirer son consentement.

Suite aux recommandations de votre Commission sur le consentement multi-terminaux, il serait même intéressant d'insérer dans cette recommandation sur la preuve de consentement une obligation de « tableau de bord du consentement », disponible facilement aux utilisateurs authentifiés, et rappelant tous les cookies consentis au travers du temps et des périphériques, pour leur permettre simplement de cesser d'y consentir ou tout simplement d'en être aisément informés.

Il sera rappelé que le RGPD impose aux Responsables de Traitement, et non à la Personne Concernée, de s'assurer de pouvoir disposer d'une preuve de consentement. Dans le cas contraire, le traitement est tout simplement illicite.

La CNIL reconnaît elle-même dans sa recommandation qu'une telle preuve est en pratique techniquement impossible (« *En effet, dans la plupart des cas, l'utilisation de traceurs a lieu dans un contexte où l'utilisateur n'est pas précisément identifié et où l'identifier de manière pérenne rendrait le traitement beaucoup plus intrusif que nécessaire.* »).

Nous ne pouvons que confirmer cet état fait, puisqu'au travers de multiples demandes d'accès, même en possédant les cookies déposés et en les transmettant aux Responsables de Traitement, ils sont dans l'incapacité de retrouver les traces de consentement ou de communiquer les traitements réalisés[11].

> Le constat est sans appel : la quasi-totalité des sites audités contrevient à la législation en vigueur, et généralement à l'ensemble des obligations légales plus qu'à des manquements mineurs.

[11] Courtiers en données : l'identification est possible pour vendre des publicités, non pour exercer les droits fondamentaux.

Cependant, nous divergeons de la CNIL en ce que nous ne voyons aucune raison d'adopter toujours plus d'exceptions aux traitements liés à des cookies alors qu'ils devraient au contraire totalement disparaître, puisque légalement impossibles à mettre en œuvre.

Une nouvelle fois, notre Association s'oppose à un nivellement par le bas, voire à une disparition pure et simple, des droits des Personnes Concernées au seul motif de l'existence de traitements mis en œuvre par des Responsables de Traitement incapables de trouver des implémentations licites. De telles implémentations, illicites par nature même, devraient être sanctionnées et interdites, et non exemptées au travers d'une recommandation de votre Commission.

7. Sur le recueil de consentement par un tiers (§3.4)

Pour éviter une incompréhension feinte des Responsables de traitement, La notion de « cookies tiers » devrait être explicitée, par exemple en ajoutant, entre parenthèses : « *exemple : le site web de l'éditeur X collecte le consentement pour les cookies déposés par la régie publicitaire Y* ».

La CNIL devrait préciser que le contrat doit préciser les conditions *et les modalités* de mise à disposition des éléments de preuve.

Au dernier paragraphe, la CNIL devrait ajouter : « *Inversement, le tiers collecteur informe sans délai le Responsable de traitement qu'il ne lui a pas communiqué les conditions, modalités et mécanismes pour lui transmettre les preuves de consentement. Cette information doit permettre au Responsable de traitement de prendre les mesures appropriées tant pour remédier aux non-conformités constatées que pour prévenir leur survenue ou leur réitération* »

Nous attirons encore une fois l'attention de la CNIL sur la nécessité d'une vigilance accrue en cas de contrôle ou d'instruction par ses services dans de tels cas.

Comme indiqué précédemment, les cas sont fréquents d'usurpation de consentement au travers d'une chaîne parfois longue (primo-collectant, courtier, ré-utilisateur) conduisant à du blanchiment de données à caractère personnel.

8. Sur la conservation de la preuve du consentement (§4)

La CNIL devrait préciser, et/ou chiffrer, et/ou illustrer par des exemples, et/ou borner les durées de conservation après la fin du traitement. Quelle durée maximale pour la constatation / l'exercice / ou la défense d'un droit ? Identique entre une lettre d'information et un service plus engageant ? À quelles obligations légales pense la CNIL ?

En l'état, la CNIL ne fait que paraphraser le RGPD et les lignes directrices 05/2020 du CEPD, ce qui n'a aucun intérêt, les Personnes concernées et les DPO de bonne foi, toutes deux à la recherche d'information, notamment pour argumenter face à un Responsable de traitement, ne sont pas plus avancées.

La CNIL ne peut pas, d'un côté, « *relev[er] des difficultés rencontrées par certains responsables de traitement pour déterminer les durées de conservation* »[12], et, d'un autre côté, persister à adopter des recommandations imprécises et insipides.

Pour l'association PURR

[redacted] Membre du Conseil d'administration

[redacted] Membre du Conseil d'administration

[redacted]

[redacted]

12. https://www.cnil.fr/fr/droit-effacement-bilan-cnil-action-europeenne