Réponse à consultation
Outils de rejeu de session

Association PURR

22 avril 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 (PC, 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 consultation de la CNIL sur son projet de recommandation relative aux outils de rejeu de session.

Table des matières

1. Généralité

L'expression « projet de recommandation » apparaît dans le titre du document, au point 5, et dans le titre de la section 3 (« Périmètre du projet de recommandation »).

Nous invitons la CNIL à ne pas oublier ces occurrences dans la version finale.

2. Sur l'introduction (§1)

Concernant le point 2 : comme indiqué lors de la concertation, le cas d'usage « diagnostic d'erreurs techniques » n'est pas le plus pertinent pour illustrer les outils de rejeu de session en ce qu'il existe des outils moins intrusifs, comme les outils de collecte, d'observation et de suivi d'événements techniques (ex. : Sentry, GlitchTip, etc.).

De même, cette finalité est distincte de la mesure d'audience au sens courant, donc il est inexact de parler de remplacement de l'un par l'autre.

Ces indications peuvent avoir un effet incitatif sur les Responsables de traitements (RTs).

Nous invitons la CNIL à clarifier cette phrase en choisissant un cas d'usage plus pertinent et en ne le liant pas mal à propos à une technique pré-existante.

3. Sur le périmètre (§3)

Nous invitons la CNIL à reformuler son encart « exemple » afin que l'éditeur (ici l'entité B) soit le sujet des actions. Exemple : la société A (éditeur) recourt à la solution de rejeu de session fournie sous forme de logiciel en tant que service par la société A (fournisseur) afin de détecter des problèmes techniques sur son site internet.

4. Sur les finalités (§4)

Concernant le point 15, PURR réitère sa position lors de la concertation : les finalités exposées peuvent être atteintes de manière raisonnablement aussi efficace par des moyens moins attentatoires à la vie privée (CJUE C-439/19, pt. 110 ; C-708/18, pt. 47), donc **les outils de rejeu de session ne sauraient être utilisés pour ces finalités**. Cette recommandation est donc dénuée d'objet.

La détection d'une erreur technique peut être mise en œuvre via des outils de collecte, d'observation et de suivi d'événements techniques (ex. : Sentry, GlitchTip, etc.), de l'analyse des journaux applicatifs (logs), ou par un signalement de la PC au service

assistance. Les exemples avancés par les RTs durant la concertation, comme le diagnostic de la présence de caractères non-alphanumériques dans l'adresse de courriel saisie dans un formulaire web, ne sont guère convaincants (il suffit de respecter la norme RFC 5322 et d'autoriser l'ensemble des caractères prévus). Lors de la concertation, la CNIL attendait que les RTs participants lui communiquent des usages plus à même de justifier le recours au rejeu de session. La société civile, et en tout cas PURR, n'a pas été informée de la suite.

L'amélioration de l'expérience utilisateur peut être mise en œuvre par du test A/B, les retours clients, ou, pour les refontes majeures d'un site web ou d'une application mobile, par un panel de testeurs. En tout état de cause, **la CNIL doit ajouter** à l'encart de fin de section, au-delà du reciblage publicitaire, l'ensemble des traitements à visée purement marketing qui vont au-delà de l'expérience utilisateur, comme la conception d'interfaces addictives ou trompeuses, ou l'analyse des émotions et des biais sur un site web, *cf.* igonogo[1].

L'assistance peut être mise en œuvre par une véritable prise en charge humaine qui permet, par exemple, de réitérer la démarche, comme passer une commande, en étant guidé par téléphone ou messagerie instantanée. Un outil de suivi des erreurs techniques pourra, en complément, permettre de s'assurer que l'utilisateur n'est pas victime d'un dysfonctionnement technique.

Au point 17, la CNIL devrait préciser que les finalités du point 15 ne sont pas intrinsèquement conformes à la réglementation du seul fait de figurer dans cette recommandation, mais que cette conformité dépend de leur mise en œuvre *effective*.

5. Sur les modalités de recueil du consentement (§5.2)

Au point 21, la CNIL devrait rester plus générale, ne pas évoquer uniquement les CMP, notamment car sa recommandation s'applique aussi au rejeu de session sur applications mobiles : « Le consentement des utilisateurs peut être recueilli par le biais des interfaces usuelles permettant un recueil valable du consentement, dont les CMP ».

1. https://igonogo.io/

Une erreur matérielle s'est glissée au point 22 : dans « les utilisateurs doivent recevoir une information conforme à cet article », il devrait être écrit « ces articles » puisqu'il est question des articles 13 et 14 du RGPD.

PURR s'oppose vivement au point 23.

D'une part, la doctrine de la CNIL a toujours été que la présentation synthétique de chaque finalité des cookies et autres traceurs doit figurer au premier niveau, et non pas au deuxième. La CNIL a appliqué cela dans les récentes réclamations 44-102503, 44-94295, 44-94293, 44-94378, 44-94383 portées par notre Association : « *l'internaute doit disposer, au premier niveau d'information […], a minima des informations relatives : […] aux finalités de chacune des opérations de lecture et/ou d'écriture effectuées sur son terminal (c'est-à-dire qu'il convient d'indiquer clairement en quelques mots à quoi servent les traceurs)* ». Rien ne justifie qu'il en soit différemment dans le cas d'espèce, notamment parce que, comme le consigne la CNIL aux points 18 et 25, le fonctionnement des cookies et autres traceurs, ainsi que l'existence du rejeu de session, échappent au grand public.

D'autre part, l'information délivrée à travers les modèles de messages, qui bien qu'indicatifs sont incitatifs, n'est pas représentative du traitement et de sa portée, notamment de son caractère intrusif, donc elle ne permet pas un consentement éclairé. En effet, dans une application mobile, cela revient à filmer l'écran, et, d'une manière générale, à capturer les interactions entre une personne et un site web, ce qui est très différent d'un suivi d'erreur technique ou des autres finalités usuelles des traceurs. Il faut donc informer de cela, de cette différence, en langage clair et sans détour. Par sa nature et sa faible connaissance par le grand public (*cf.* point 25), le rejeu de session ne peut pas être noyé ni confondu au sein d'une même finalité avec d'autres outils moins attentatoires à la vie privée, comme le suivi d'erreur technique.

PURR s'oppose vivement au point 24 : comme il vient d'être dit, l'information *doit* être spécifique aux outils de rejeu de session et elle *doit* figurer au premier niveau. Ce n'est pas une option ni une bonne pratique, mais bien une obligation légale. Peu importe les finalités et les mesures mises en œuvre : ces dernières sont aussi une obligation légale,

pas une option, donc leur mise en œuvre est due et n'influe pas sur l'information qui doit être délivrée.

Une nouvelle fois, il revient aux RTs de minimiser et de supprimer si nécessaire les traitements mis en œuvre s'ils souhaitent conserver une CMP de premier niveau simple. Il ne revient pas à la CNIL de tolérer de plus en plus le report au second niveau d'une information légalement obligatoire au premier niveau, au seul motif que la CMP en deviendrait trop complexe.

À ce sujet, la CNIL *doit* exposer que le traitement subséquent, c'est-à-dire la capture et la restitution des interactions entre une personne et un site web, doit figurer, avec toutes les mentions obligatoires, dans les autres informations délivrées au titre de l'article 13 du RGPD (souvent une politique de confidentialité ou de protection des DCP).

La CNIL **doit préciser** qu'en application du principe de minimisation, l'outil de rejeu de session ne doit pas être téléchargé dans le navigateur web des visiteurs du site web de l'éditeur tant que ceux-ci n'ont pas consentis. Nous ne parlons pas d'activation, mais bien de téléchargement. Ce dernier constitue un inutile transfert de DCP vers le fournisseur (adresse IP, marque, modèle, et version de navigateur web et de système, provenance, langue, date+heure, etc.) qui permet de tirer des conclusions très précises sur la vie privée de la personne, notamment si le fournisseur est présent sur de nombreux sites web ou en fonction du caractère médical, syndical, philosophique, religieux, etc. du site web de l'éditeur, alors que le transfert n'est pas nécessaire en l'absence de consentement.

6. Sur les traitements subséquents (§5.3)

D'abord, le titre de la section, et la section elle-même, sont incomplets et ambigus puisque le fournisseur peut aussi mettre en œuvre des traitements subséquents, *cf.* pt. 10. De même, le traitement principal, c'est-à-dire la capture d'une session de navigation, sera *effectivement* mis en œuvre par le fournisseur pour le compte de l'éditeur. La CNIL doit donc prévoir un titre et une section plus générales.

Ensuite, **PURR s'oppose vivement au point 29** : compte-tenu de son caractère hautement intrusif (comportement de la personne, mouvements de souris, etc.),

notamment sur mobile, le principal traitement subséquent ne peut reposer que sur le consentement. De même, comme il a été dit supra, il ne s'agit pas de recueillir simultanément le consentement à la finalité et aux traceurs, mais également à la technologie de rejeu de session.

Enfin, la CNIL *doit* rappeler qu'en cas de mobilisation de l'intérêt légitime, l'éditeur et/ou le fournisseur (dans le cas de l'amélioration de l'outil, par ex.) doivent permettre un **exercice facile[2] du droit d'opposition** (article 21 du RGPD) et qu'aucune des finalités exposés dans la recommandation ne relève d'un motif impérieux susceptible d'y faire obstacle.

7. Sur les traitements ultérieurs (§5.4)

Concernant le point 32, nous demandons à la CNIL de, d'une part, renvoyer à sa documentation sur l'anonymisation *effective* des DCP[3] et/ou de rappeler que l'anonymisation suppose une résistance à l'identification, à la corrélation et à l'inférence, et, d'autre part, qu'en l'espèce, compte-tenu de la capture des interactions entre une personne et un site web, l'anonymisation est très difficile, notamment sur mobile (puisque nous sommes en présence d'un enregistrement vidéo sur lesquels les fournisseurs n'arrive déjà pas à masquer des champs).

8. Sur la preuve du consentement (encart page 9)

En préambule, la bonne place de cet encart n'est pas « dans » la section relative aux traitements ultérieurs, mais dans une section dédiée qui, de surcroît devrait être située en amont, après la section 5.2, par exemple. Nous invitons donc la CNIL à repositionner la preuve du consentement.

De même, l'encart contient une ambiguïté : il n'y a pas de « paragraphe 48 » dans la version consolidée[4] de la recommandation relative aux cookies et autres traceurs. En correction, la CNIL pourrait utilement pointer l'article 4 de ladite recommandation.

Enfin, PURR s'étonne vivement de la présence de cet encart alors que la preuve du consentement, y compris l'exception en matière de traceurs, fait, depuis fin janvier 2026,

---

2. https://www.cnil.fr/fr/gestion-des-cookies
3. https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles
4. https://www.cnil.fr/fr/cookies-et-autres-traceurs-recommandations-finales-sur-le-consentement-multi-terminaux

l'objet d'une concertation dédiée. Cela signifierait-il que cette concertation n'a aucun intérêt, et que les décisions ont déjà été prises ? Pour clarifier cela, PURR demande à la CNIL de reporter la publication de la recommandation rejeu de session à la fin des travaux sur la preuve de consentement ou, sinon, de retirer cet encart de la version finale.

Sur le fond, **PURR s'oppose vivement à une preuve de procédé**, réitère sa position sur la non-conformité d'une telle preuve et renvoie à la section 6 de sa contribution écrite du 6 mars 2026 dans la concertation sur la preuve de consentement.

En substance, la preuve du consentement a été conçue comme une protection d'une PC contre un traitement de ses DCP faussement ou prétendument fondé sur son consentement. Cette garantie serait vidée de sa substance si elle ne s'appliquait pas à un traitement aussi intrusif que le rejeu de session ou à l'expression la plus courante du consentement que constitue celui aux traceurs. Or, une disposition de droit souple ne saurait vider de sa substance une norme juridique de rang supérieur, à supposer que la CNIL ait compétence pour l'édicter, ce dont PURR doute.

Au point 108 de ses lignes directrices 5/2020, le CEPD rejette la preuve de procédé. La future recommandation ne doit pas conduire à une fragmentation de l'application du droit de l'UE.

Un éditeur de site web dispose *déjà* des éléments de preuve du consentement : identifiant de session, et/ou horodatage, et/ou journal de sa CMP dont interactions et/ou données soumises (ex. : TC String), et/ou informations de contexte (adresse IP, User-Agent, etc.), etc. Point besoin d'une identité civile, ou d'un compte utilisateur, ou d'une association entre tout ça, il s'agit seulement de donner matière à contestation d'un consentement forgé ou usurpé.

La force de la preuve peut être adaptée au contexte (environnement authentifié ou non, DCP collectées pour rendre le service demandé par l'utilisateur, etc.), mais le dilemme exposé lors de la concertation orale sur le rejeu, entre un identifiant unique, plus intrusif mais permettant l'exercice des droits RGPD, et un identifiant aléatoire plus protecteur qui annihile les droits, est un faux dilemme, une construction factice.

9. Sur l'exercice des droits (§6)

Comme il a été dit supra, si d'autres bases légales sont possibles, *cf.* pt 29, alors la CNIL doit lister le droit d'opposition au point 33, y consacrer une sous-section, similaire à la section 6.2, relative à ses conséquences, exiger la simplicité de cette opposition (comme pour les cookies de mesures d'audience)[5], et rappeler qu'aucune des finalités exposés au point 15 ne justifie d'un intérêt impérieux susceptible d'y faire obstacle.

La CNIL doit rappeler qu'en cas de responsabilité conjointe (si le fournisseur poursuit également ses propres finalités), l'éditeur et le fournisseur doivent définir contractuellement qui traite les exercices de droits, notamment l'opposition aux traitements mis en œuvre par le fournisseur pour son propre compte.

La CNIL doit rappeler le point 117 des lignes directrices 5/2020 du CEPD : quand le consentement est retiré, l'éditeur doit arrêter tout traitement des données d'interaction collectées sous le régime de ce consentement, et supprimer ces données (conformément à l'article 17(1)b du RGPD). Idem en cas d'opposition (article 17(1)c du RGPD). Il est improbable qu'aucune association n'existe entre un cookie retiré ou opposé et des captures (= données d'interaction).Là encore, il n'y a pas besoin de collecter des DCP en sus ni d'associer les données d'interaction à l'identité civile ou au compte utilisateur du visiteur.

Sur ce dernier point, nous rappelons que, bien évidemment, l'exercice des droits peut être adapté aux DCP détenues par l'éditeur et au contexte (environnement authentifié ou non, par ex.). s'il existe nativement, pour poursuivre la finalité, une association entre les données d'interactions et un compte utilisateur voire une identité civile, comme c'est le cas dans l'usage « assistance aux utilisateurs », alors l'éditeur doit satisfaire les droits RGPD à partir de la référence du compte utilisateur. Inversement, dans un cas d'usage sans association, comme « l'amélioration de l'expérience utilisateur », la PC désireuse d'exercer ces droits pourrait avoir à fournir des DCP pertinentes supplémentaires (identifiant du cookie rejeu de session, adresse IP, horodatage, etc.), et l'éditeur devrait la guider en ce sens. En tout état de cause, un éditeur, comme tout RT, ne saurait refuser un exercice de droit lorsque les données lui permettant d'y satisfaire lui sont communiquées[6].

---

5. https://www.cnil.fr/fr/gestion-des-cookies
6. https://noyb.eu/en/data-brokers-identification-possible-sell-ads-not-exercise-fundamental-rights

10. Sur les principes de protection des DCP (§7)

PURR demande vivement à la CNIL de **reformuler le point 37 de la sorte** : « La configuration des outils de rejeu de session doit permettre aux éditeurs de respecter l'ensemble des principes et dispositions du RGPD, notamment les principes de minimisation, de limitation des durées de conservation et de sécurité des traitements de données personnelles. ».

De même, la CNIL doit préciser que les recommandations à suivre viennent préciser l'état de l'art et l'ensemble de la documentation mise à disposition par la CNIL et l'ANSSI et que, ce faisant, **la protection des DCP ne se résume pas aux mesures énoncées** dans la présente recommandation.

Au point 38, afin de renforcer son propos, la CNIL pourrait utilement pointer vers le considérant 81 du RGPD et ses articles 24(1) et 28(1).

11. Sur le principe de minimisation (§7.1)

PURR demande à la CNIL de débuter cette section par un rappel que des solutions moins attentatoires à la vie privée doivent être privilégiés dès qu'elles permettent d'atteindre la finalité poursuivie de manière raisonnablement aussi efficace (CJUE C-439/19, pt. 110 ; C-708/18, pt. 47).

La CNIL pourrait utilement donner un autre exemple pour L3 : la fin de la prise en charge d'un utilisateur par le service assistance entraîne la suppression des données.

Concernant le point 43.

D'abord, PURR demande à la CNIL d'ajouter qu'en premier lieu, le masquage devrait, par défaut, conduire à la non-collecte, par le fournisseur, d'un champ de saisie ou d'un emplacement donné. Ce n'est que dans un deuxième temps qu'il peut être envisagé une collecte par le fournisseur couplée à une absence de restitution à l'éditeur (sauf circonstances développées dans le projet). Cela avait été plébiscité par l'ensemble de la société civile lors de la concertation.

Ensuite, PURR s'oppose vivement à la sélection automatique des emplacements dans lesquels il ne doit pas y avoir de collecte ou de restitution à l'éditeur. A minima, la CNIL doit exiger une validation manuelle des conséquences de la sélection automatique.

De plus, la CNIL doit préciser que, par défaut, en absence de configuration, l'absence de collecte ou de restitution s'applique à toutes les catégories, donc à tous les champs de saisie.

De même, la CNIL doit rappeler que l'occultation par défaut de l'ensemble d'un formulaire est nécessaire en ce que l'apparence même d'un formulaire web peut révéler des DCP sensibles en réaction à un clic. Exemple : des nouvelles options ou de nouveaux champs ou cases à cocher ou… qui n'apparaissent qu'en réaction à un choix précis antérieur. Il en va de même des champs de texte libre qui, dès lors, doivent faire l'objet d'une vigilance particulière.

Enfin, la CNIL doit préciser M1 : le processus interne de validation de la demande de démasquage implique-t-elle un supérieur hiérarchique (UX ou diagnostic des erreurs techniques) ou l'utilisateur (cas de l'assistance dans le tableau de l'annexe 1) ou les deux ?

Au point 44, la CNIL pourrait utilement rappeler qu'un identifiant aléatoire ne signifie pas anonyme, notamment si un lien est fait avec un cookie ou traceur, et renvoyer au point 32.

12. Sur la limitation de la conservation (§7.2)

PURR constate l'absence de préconisation en ce qui concerne la durée du consentement au rejeu de session (= de la collecte des données d'interaction), c'est-à-dire, in fine, de la durée de vie du cookie / traceur qui stocke ledit consentement.

Interrogée lors du troisième atelier de la concertation, la CNIL avait répondu que la durée était alignée sur celle des cookies usuels. l'ensemble des représentants de la société civile avait exprimé que cette durée de 6 mois, est excessive en ce qu'il constitue une apparence de consentement infini.

Nous demandons à la CNIL d'expliciter la durée du consentement et des traceurs de rejeu de session, et de la borner en fonction de la finalité poursuivie (par exemple : « quelques heures » pour l'assistance aux utilisateurs).

13. Sur la sécurité (§7.3)

Nous invitons la CNIL à corriger la coquille du point 48 : « mise en œuvre en œuvre ».

14. Annexe 1 (§8)

D'abord, nous demandons à la CNIL d'ajouter une colonne qui, pour chaque finalité, rappellerait des alternatives moins attentatoires aux outils de rejeu de session. Nous en avons énuméré certaines ci-dessus en réaction au point 15 du projet.

Concernant l'assistance aux utilisateurs, la CNIL doit ajouter L3 (la résolution du problème par le service assistance conduit à la suppression des données d'interactions) et définir une durée maximale de 8 heures (= une journée de travail).

Concernant l'expérience utilisateur : la CNIL doit préciser que le recours au rejeu de session doit être ponctuel (après le déploiement d'une nouvelle version du site web ou de la détection d'une anormalité) et que l'éditeur doit procéder par échantillonnage parmi les personnes ayant consenti. La CNIL doit borner la conservation à trois mois (après le déclenchement d'une campagne, *cf.* ponctualité) et à 8 heures après la première exploitation (cela laisse le temps de retranscrire ce qui ne va pas et/ou de le reproduire sur la version de test), le minimum l'emportant.

Concernant le diagnostic des erreurs techniques : la CNIL doit laisser M1 uniquement si la validation de l'accès aux données masquées provient d'un supérieur hiérarchique (*cf.* supra), pas du premier informaticien venu. La CNIL doit borner la conservation à 3 mois et à 8 heures après la première exploitation, le minimum l'emportant.

Pour l'association PURR

[redacted]

Membre du Conseil d'administration

[redacted]

[redacted]

Membre du Conseil d'administration

[redacted]