PROJET DE RECOMMANDATION

concernant les outils de rejeu de session

Document soumis à consultation publique jusqu'au 22 avril 2026

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Table des matières

1. Introduction

1. Les outils de rejeu de session sont des technologies de capture et de visualisation du parcours complet de navigation d'un utilisateur de site web ou d'application mobile. Ils permettent, au-delà de la collecte d'informations concernant les pages ou écrans visités, de visionner l'ensemble des actions de navigation, telles que les mouvements de souris, clics ou interactions tactiles, défilement des pages, saisies de l'utilisateur et autres interactions.

2. Ces outils sont utilisés par des éditeurs de sites web et d'applications mobiles car ils permettent des analyses précises de la navigation des utilisateurs. Via le rejeu de la navigation des utilisateurs, les éditeurs bénéficient de données détaillées qui expliquent les parcours de navigation. Ces données sont utilisées pour répondre à certains cas d'usage (par exemple, détecter et comprendre des erreurs ou problèmes techniques) en remplacement de mesures plus classiques (par exemple, les outils de mesure d'audience ou « *analytics* »).

3. L'**utilisation de ces outils peut présenter certains risques**. D'une part, ils peuvent conduire à un suivi permanent de la navigation permettant de disposer d'informations précises sur la vie privée des personnes (habitudes, centres d'intérêts, données sensibles dans certains cas, etc.). D'autre part, ils peuvent entrainer une collecte excessive de données ne répondant pas à l'obligation de proportionnalité au regard de la finalité initialement envisagée. Le niveau de risque dépend généralement de la nature du site web ou de l'application mobile visités.

4. Ces risques sont d'autant plus importants qu'il existe de nombreux modèles d'affaires comportant la commercialisation d'outils de rejeu de session et proposant des fonctionnalités et paramétrages variés. Leur diversité accroît les choix disponibles pour les éditeurs de sites web et d'applications mobiles et contribue à maintenir un rythme rapide d'évolution technique de ces outils. Ainsi, les éditeurs peuvent être incités à avoir recours à des fonctionnalités et paramétrages qui permettraient d'accéder à davantage d'informations sur les parcours des utilisateurs.

5. La CNIL considère donc qu'il est nécessaire **d'encadrer l'usage croissant des solutions de rejeu de session. Le projet de recommandation propose des recommandations pratiques aux fournisseurs qui proposent ces outils et aux éditeurs qui les exploitent afin de s'assurer du respect de la règlementation applicable.** Ce projet de recommandation n'est pas exhaustif et ne présente pas de caractère règlementaire. Il a pour seul objectif d'aider les professionnels concernés dans leur démarche de mise en conformité. Il a été élaboré à la suite d'une phase de concertation avec des représentants des professions concernées par l'usage de ces outils, d'une part, et des représentants de la société civile, d'autre part.

2. Cadre légal applicable

6. **En premier lieu**, les outils de rejeu de session impliquent des traceurs permettant la réalisation d'opérations de lecture et d'écriture d'informations auxquelles s'appliquent les **principes et obligations posés par l'article 82 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** (« **loi informatique et libertés** ») qui transpose l'article 5.3 de la directive n°2002/58/CE dite « vie privée et communications électroniques ».

7. **En second lieu**, ces outils reconstituent des sessions individuelles de navigation : ils permettent la collecte de données identifiant directement ou indirectement les utilisateurs, quels que soient leur configuration et les paramétrages utilisés. Ces traitements, basés sur des données produites ou collectées via un traceur (aussi appelés « les traitements subséquents »), doivent respecter **le règlement général sur la protection des données (RGPD) et la loi « informatique et libertés ».**

3. Périmètre du projet de recommandation

3.1 Environnements Technologiques concernés

8. Les outils de rejeu de session permettent de suivre la navigation des utilisateurs sur un site web ou une application mobile. Ces outils fonctionnent avec des traceurs (qui peuvent être des cookies dans le contexte du web, ou d'autres technologies comme par exemple les identifiants mobiles au sein des applications mobiles). Ils permettent la visualisation de **sessions reconstituées,** soit à partir de données d'interaction avec un site web ou une application mobile, soit à partir de la lecture d'**enregistrements de sessions** de navigation.

3.2 Les qualifications des acteurs concernés en vertu du RGPD

9. Cette recommandation s'applique aux éditeurs de sites web et d'applications mobiles et aux fournisseurs d'outils de rejeu de session établis en France ou sur le territoire de l'Union Européenne ou encore à ceux mettant en œuvre des traitements de données à caractère personnel qui concernent des personnes situées au sein de l'Union Européenne conformément à l'article 3 paragraphes 1) et 2) du RGPD et aux dispositions pertinentes de la loi « informatique et libertés ». Chacun de ces acteurs doit déterminer son rôle au regard du traitement réalisé.

Le fournisseur des outils de rejeu de session

10. Il s'agit de l'entreprise qui fournit la **solution technique** de rejeu de session. Elle définit les paramétrages disponibles de l'outil mis à disposition des éditeurs. La qualification de cet acteur dépend des finalités qu'il poursuit conjuguées avec la nature des données qui sont issues de l'outil :

- lorsqu'il fournit l'outil à l'éditeur sans réutiliser les données collectées pour ses propres finalités, le fournisseur agit en tant que **sous-traitant** ;

- **si le fournisseur, avec l'accord de l'éditeur, utilise les données collectées par l'outil pour ses propres finalités** (par exemple, afin d'améliorer la solution fournie) il est seul **responsable du traitement au sens du RGPD** à l'égard **de ces traitements subséquents**. Le fournisseur est également **responsable conjoint de l'éditeur** pour les opérations de lecture et d'écriture à l'origine de ces traitements[1].

[1] cette responsabilité conjointe s'inscrit dans la lignée de la jurisprudence Fashion ID (§101 et 102) et des lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (§38).

Conformément à l'article 26 du RGPD, cette relation suppose une répartition claire et transparente des obligations notamment en matière d'information des personnes concernées et de respect de leurs droits.

L'éditeur de site web ou d'applications mobiles

11. L'éditeur désigne l'acteur (entreprise, organisme public, etc.) qui choisit d'utiliser un outil de rejeu de session sur son site web ou sur son application mobile. **Il est généralement considéré comme responsable du traitement** car il décide de recourir à un outil qui a pour objectif de satisfaire un besoin qui lui est propre. Il détermine, de ce fait seul la ou les finalité(s) qu'il poursuit et, en paramétrant l'outil, il participe à la détermination des moyens essentiels de ses traitements.

12. **L'éditeur est seul responsable des opérations de lecture et d'écriture réalisées exclusivement pour son compte** à savoir celles permettant la collecte de données qui sont ensuite traitées uniquement pour ses finalités.

Exemple

La société A (fournisseur de la solution) fournit une solution de rejeu de session comme un logiciel en tant que service (*Software as a service* ou SaaS) à la société B (éditeur) afin que celui-ci puisse détecter des problèmes techniques sur son site internet. La société A prévoit, avec l'accord contractuel de la société B, d'utiliser les données de navigation recueillies afin d'améliorer le fonctionnement de son outil. Les qualifications respectives sont réparties de la manière suivante :

- **S'agissant du traitement mis en œuvre par la société B à des fins de détection de problèmes techniques de son site internet :** l'éditeur est responsable du traitement et la société A est sous-traitant ;

- **S'agissant des traitements mis en œuvre par la société A pour améliorer ses services :** la société A est responsable du traitement indépendant car il s'agit de traitements mis en œuvre à des fins propres ;

- **S'agissant des opérations de lecture et d'écriture mis en œuvre pour la collecte des données** : étant donné que les données ainsi collectées servent les finalités des deux sociétés, celles-ci sont responsables conjointement de ces opérations.

4. Objectif(s) poursuivi(s) par le traitement (finalités)

13. Les outils de rejeu de session peuvent être utilisés pour différentes finalités, qui doivent être **déterminées, explicites et légitimes**.

14. Elles doivent être définies par le responsable du traitement (éditeurs ou fournisseurs) **en amont du déploiement de l'outil**. Elles ne peuvent être déterminées **postérieurement** à la collecte des données, ni **dépendre de ce que le responsable du traitement** est amené à visualiser grâce à l'outil.

15. L'outil peut être déployé par les éditeurs sur leurs sites web ou applications mobiles pour les finalités suivantes :

    - **détection et compréhension des erreurs ou problèmes techniques :** la visualisation de session(s) individuelle(s) de navigation permet d'identifier des erreurs techniques et de les résoudre à partir d'éléments de navigation obtenus en situation réelle et non détectables au moyen de métriques d'analyse classiques ;
    - **amélioration de l'expérience utilisateur (« UX »)** : la visualisation de session(s) individuelle(s) de navigation affine la connaissance du parcours utilisateur en révélant des comportements non détectables au moyen de métriques d'analyse classiques et permet l'identification de zones de frictions (clics causés par l'énervement de l'utilisateur, faux clics, etc.), de fluidifier la navigation ou encore d'améliorer l'ergonomie du site ou de l'application ;
    - **support et assistance pour gérer les demandes client (ou problème avec les services proposés)** : la reproduction de sessions propres à un utilisateur ayant rencontré un problème lors de sa navigation permet au responsable du traitement de mieux répondre aux demandes qu'il est susceptible de recevoir (par exemple, lorsqu'un utilisateur ne parvenant pas à valider sa commande contacte le service client).

16. Selon la ou les finalités recherchées, une attention particulière doit être portée au **paramétrage de l'outil :** le choix des fonctionnalités dépend de chaque finalité.

17. Le responsable de traitement qui utilise un outil de rejeu de session pour d'autres finalités que celles identifiées dans cette recommandation doit s'être assuré de la conformité d'un tel usage à la réglementation.

> Conformément au principe de minimisation (article 5.1.b du RGPD), et au vu des risques inhérents au rejeu de session, le responsable de traitement devra privilégier l'usage d'outils alternatifs, traitant moins de données, s'ils permettent de réaliser les mêmes objectifs. Par exemple, un outil de rejeu de session ne devrait pas être utilisé à des fins de reciblage publicitaire, compte tenu de l'existence de solutions plus respectueuses de la vie privée (par exemple, des cookies de relance « panier »).

5. Information et consentement

18. L'information est un des critères de licéité du consentement éclairé (articles 4.11, 6.1.a du RGPD). Les responsables du traitement doivent être particulièrement vigilants sur ce point, d'autant plus que le fonctionnement des technologies de cookies et traceurs est bien souvent peu connu du grand public, qui ne peut pas toujours détecter leur utilisation.

5.1 La nécessité d'un consentement conformément à l'article 82 de la loi « informatique et libertés »

19. Sauf exemption, les opérations de lecture et d'écriture de toute information stockée ou consultée dans un équipement terminal nécessitent le recueil du consentement. Les finalités poursuivies par le déploiement des outils de rejeu de session sont soumises au consentement préalable des utilisateurs. En effet, les opérations de lecture et d'écriture :

- n'ont pas pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- ne sont pas strictement nécessaires à la fourniture des services proposés par les éditeurs, puisque ces derniers pourraient les fournir sans elles.

20. Ce consentement doit être recueilli dans les conditions rappelées à l'article 2 des lignes directrices[2] et l'article 2 de la recommandation « cookies et autres traceurs »[3], sous réserve des recommandations spécifiques ci-dessous.

5.2 Les modalités pratiques de recueil du consentement

Utilisation des outils déjà déployés pour recueillir le consentement

21. Le consentement des utilisateurs peut être recueilli par le biais des plateformes de gestion des consentements (*consent management platform* ou CMP) déployées par les éditeurs sur leurs sites ou leurs applications. Ces plateformes devront, le cas échéant, être mises à jour afin de respecter les exigences découlant du droit positif applicable, explicitées par les recommandations suivantes.

22. Les responsables du traitement doivent veiller à mettre à jour les documents d'information et de recueil du consentement qu'ils mettent à disposition des personnes concernées (module de gestion des cookies, mentions d'informations dédiées, CMP, etc.), conformément aux obligations que leur imposent les articles 13 et 14 du RGPD. Pour mémoire, lorsqu'aucune des exemptions prévues à l'article 82 de la loi « Informatique et Libertés » n'est applicable, les utilisateurs doivent recevoir une information conforme à cet article, complétée le cas échéant par les exigences du RGPD (destinataires des données, durées de conservation, etc.).

Informations nécessaires pour recueillir un consentement éclairé

23. Chaque finalité pour laquelle l'outil est déployé doit être présentée aux utilisateurs, avant que ceux-ci soient mis en mesure de consentir ou non, dans un intitulé court, accompagné d'un bref descriptif susceptible de leur permettre de comprendre la portée de leur choix. À titre d'exemples, pour les finalités présentées précédemment, le deuxième niveau d'information des CMP, au regard des exigences encadrant le recueil du consentement, a vocation à présenter les informations suivantes :

- **Détection et compréhension des erreurs ou problèmes techniques :** *[Nom de l'éditeur] utilise des traceurs (outils d'enregistrement du parcours utilisateur) pour identifier des erreurs techniques et les résoudre.*
- **Amélioration de l'expérience utilisateur (« UX ») :** *[Nom de l'éditeur] utilise des traceurs (outils d'enregistrement du parcours utilisateur) pour identifier des zones de friction dans les parcours de navigation afin de fluidifier la navigation et d'améliorer l'ergonomie du site [ou de l'application].*

[2] Délibération n°2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée et aux opérations de lecture et d'écriture dans le terminal d'un utilisateur (notamment les « cookies et autres traceurs ») et abrogeant la délibération n°2019-093 du 4 juillet 2019.
[3] Délibération n°2019-093 du 4 juillet 2019 et dans la délibération n°2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ».

- **Support et assistance pour gérer les demandes clients (ou problèmes avec les services proposés) :** *[Nom de l'éditeur] utilise des traceurs (outils d'enregistrement du parcours utilisateur) pour reproduire la ou les session(s) de certains utilisateurs qui ont rencontré un problème lors de leur navigation [du site] / [de l'application], afin de répondre aux demandes que les équipes de [Nom de l'éditeur] sont susceptibles de recevoir.*

Information spécifique aux outils de rejeu de session

24. La CNIL encourage les responsables du traitement, à titre de bonne pratique, à prévoir une information spécifique concernant les outils de rejeu de session sur le premier niveau des CMP.

25. En effet, ces outils présentent certains risques et les utilisateurs de sites web ou d'applications mobiles ont une faible connaissance de leur existence et de leur fonctionnement. Chaque responsable du traitement apprécie donc, au regard de sa situation propre, l'opportunité de mettre en œuvre cette bonne pratique afin que le consentement donné soit parfaitement éclairé. La décision de porter ou non cette information sur le premier niveau des CMP doit prendre en compte l'étendue du suivi de navigation réalisé, l'impact sur les utilisateurs ainsi que les paramétrages et les mesures de minimisation mises en œuvre.

26. Cette information devrait présenter l'outil et expliquer la manière dont il fonctionne (par exemple, les données qui sont collectées et traitées, le paramétrage qui y est appliqué, etc.), afin que les utilisateurs soient réellement à même de comprendre les raisons pour lesquelles leur consentement est requis lorsqu'ils visitent un site internet ou utilisent une application mobile.

5.3 La mise en œuvre des traitements subséquents par l'éditeur

27. Les « traitements subséquents » sont les traitements qui résultent des données générées par les cookies et autres traceurs.

28. Si le principe est celui du recueil du consentement préalablement à toute opération de lecture et d'écriture d'informations sur un terminal, le traitement des données à caractère personnel issues de ces traceurs doit reposer sur une des bases légales prévues à l'article 6 du RGPD.

29. Le consentement est généralement la base légale la plus appropriée pour ce traitement subséquent mais chaque responsable du traitement doit déterminer, en fonction du contexte et de ses spécificités, celle qu'il convient de mobiliser. Lorsque la base légale du traitement subséquent est également le consentement des utilisateurs, le responsable du traitement peut le recueillir simultanément à celui qu'il recueille pour les opérations de dépôt et/ou de lecture par le biais, par exemple, d'une unique case à cocher pour chacune des finalités.

5.4 Les traitements ultérieurs des données

30. Les « traitements ultérieurs » sont les traitements définis à l'article 6.4 du RGPD.

31. Les données collectées via des opérations de lecture et d'écriture soumises au consentement de l'utilisateur ne peuvent être réutilisées pour une autre finalité qu'à la condition que l'utilisateur ait donné son consentement à cette nouvelle finalité.

32. En revanche, la réutilisation par le responsable du traitement ne nécessite pas de consentement si les données ont été préalablement anonymisées. En effet, la réutilisation de données rendues anonymes est présumée ne pas créer d'atteinte supplémentaire à la vie

privée des personnes, au regard de la protection apportée par l'article 82 de la loi « informatique et libertés ».

Preuve du recueil du consentement

Un responsable du traitement doit être en mesure de démontrer, à tout moment, que les utilisateurs ont donné leur consentement. Pour ce faire, il doit mettre en place des mécanismes qui permettent de démontrer que le consentement des utilisateurs a été valablement recueilli.

Pour les « cookies et autres traceurs », la CNIL considère que les acteurs qui se prévalent du consentement donné par l'utilisateur peuvent se limiter à apporter une preuve de procédé compte tenu des spécificités de l'environnement.

Le paragraphe 48 de la recommandation « cookies et autres traceurs » donne des exemples de mécanismes que les acteurs peuvent adopter.

Ces différents consentements peuvent être recueillis sur la CMP déployée sur le site internet de l'éditeur, quelles que soient les finalités (celles poursuivies par l'éditeur ou celles poursuivies par le fournisseur).

Lorsque les acteurs sont conjointement responsables de la collecte de ces consentements, ils ne peuvent se satisfaire de la présence d'une clause contractuelle mettant uniquement à la charge de l'éditeur l'obligation de recueillir un consentement valable pour le compte de l'autre partie.

Le contrat devrait ainsi prévoir :

- Les mécanismes mis en place pour démontrer le recueil d'un consentement valide et à qui incombe cette responsabilité.
- La mise à disposition des éléments de preuve au profit de l'organisme qui souhaite se prévaloir du consentement.
- Le cas échéant, les conditions dans lesquelles ces éléments de preuve doivent être conservés notamment afin de conserver leur valeur probante.
- Les modalités d'audits réguliers des mécanismes de recueil du consentement.

6. Exercice des droits des personnes

6.1 Généralités

33. Les utilisateurs bénéficient de droits qui leur sont garantis notamment par les articles 15 à 20 du RGPD : droit d'accès, droit à la rectification, droit à l'effacement, droit à la limitation du traitement, droit à la portabilité, etc.

34. Les responsables du traitement doivent faciliter l'exercice des droits en mettant à la disposition des utilisateurs des dispositifs ergonomiques et compréhensibles, comme par exemple un centre de gestion des droits (voir les recommandations design de la CNIL).

6.2 Conséquences du retrait du consentement

35. Les utilisateurs doivent être en mesure de retirer leur consentement à tout moment (article 7 du RGPD). Il doit leur être aussi simple de retirer leur consentement qu'il ne leur a été de le donner.

36. Les responsables du traitement doivent s'assurer de l'effectivité du retrait du consentement : les opérations de lecture et d'écriture ne peuvent plus intervenir postérieurement au retrait du consentement de l'utilisateur. Il peut être nécessaire de mettre en place des solutions spécifiques pour garantir l'absence de lecture des traceurs précédemment utilisés pour que le retrait du consentement soit considéré comme effectif (modifier la durée de vie des cookies pour signifier qu'ils sont expirés en renvoyant dans une réponse http un en-tête « set cookie » approprié spécifiant une date d'expiration dans le passé par exemple, ou encore s'agissant des cookies qui ne disposent pas de l'attribut « httpOnly », assurer leur suppression à l'aide d'un script exécuté localement sur le terminal, etc.).

7. Mise en œuvre des principes de protection des données

37. **La configuration des outils de rejeu de session doit permettre aux éditeurs de respecter les principes de minimisation, de limitation des durées de conservation et de sécurité des traitements de données personnelles.**

38. Les éditeurs **doivent choisir des fournisseurs dont les outils de rejeu de session leur permettent de respecter leurs obligations**.

39. Il s'agit pour les fournisseurs de proposer un outil paramétrable, de façon à permettre à leurs clients de prendre en compte les exigences de la règlementation et la diversité des finalités qu'ils sont susceptibles de poursuivre.

40. Ainsi, la CNIL recommande aux fournisseurs une série de mesures qui, mises à disposition des éditeurs, permettent un déploiement conforme à la règlementation. Ces mesures ne sont pas impératives et des actions alternatives peuvent être mises en œuvre dès lors qu'elles permettent aux responsables de traitement de respecter la règlementation. Il incombe alors aux responsables de traitement d'être en mesure de documenter, avec l'aide de leur fournisseur, en quoi les actions alternatives satisfont leurs obligations.

Sélection des mesures pertinentes en fonction des finalités poursuivies

Afin de guider les acteurs, la CNIL met à disposition en annexe un tableau indiquant par finalité les mesures techniques qu'il est recommandé d'appliquer.

À chaque finalité, couverte par la recommandation, correspond une série de mesures d'application cumulative ou alternative (dont le descriptif figure ci-dessous) permettant une utilisation des outils respectant les principes de la règlementation.

C'est également le rôle du fournisseur de solution, en tant que sous-traitant, de conseiller le responsable du traitement quant à la sélection des mesures pertinentes.

7.1 Assurer le respect du principe de minimisation

41. Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5.1.c du RGPD).

42. À ce titre, la CNIL recommande de **limiter les sessions collectées** en fonction de la finalité poursuivie à l'aide des fonctionnalités suivantes :

    - Echantillonnage aléatoire des sessions collectées pour limiter la quantité de données collectées (*L1*).
    - Limitation des collectes aux situations où survient un évènement déclencheur défini. Dans les situations où un historique de sessions est nécessaire, et s'il n'est pas possible de l'obtenir par d'autres moyens, est envisageable un enregistrement de l'ensemble des sessions avec suppression à bref délai des enregistrements lorsqu'aucun évènement déclencheur prédéfini n'est survenu (*L2*).
    - Analyse des sessions enregistrées et suppression à bref délai des sessions non nécessaires compte tenu de la finalité du traitement (par exemple suppression des sessions s'il est établi que l'utilisateur n'a pas rencontré de difficultés de navigation) (*L3*).

43. De plus, la CNIL recommande que soit systématiquement mis à disposition **un outil de masquage afin de limiter la nature des données mises à disposition de l'éditeur** à ce qui est nécessaire pour la finalité poursuivie : le fournisseur devrait fournir des outils adaptés pour sélectionner automatiquement et manuellement les données à ne pas rendre disponibles notamment les images, les formulaires, les champs de textes et les champs dynamiquement remplis (par exemple contenant des informations de compte). En cas d'absence de configuration, le masquage devrait par défaut s'appliquer à toutes les catégories envisagées (*M0*). De plus, l'éditeur devrait pouvoir choisir les conséquences en cas de masquage :

    - Collecte de la donnée, avec la possibilité de demander un démasquage uniquement accessible à un nombre limité d'utilisateurs habilités et un processus interne de validation de la demande (*M1*).
    - Collecte de la donnée par l'outil mais absence de mise à disposition de celle-ci à l'éditeur (par exemple via un chiffrement à la main du fournisseur). En cas de demande d'accès, celle-ci doit être motivée (*M2*).
    - Absence de collecte de la donnée (*M3*).

44. Enfin, la CNIL recommande que **l'usage d'identifiants puisse être limité** en fonction de la finalité poursuivie. L'éditeur devrait donc avoir à sa disposition les fonctionnalités suivantes :

    - Identifiant de session généré aléatoirement, dans l'objectif d'empêcher l'association de différentes sessions d'un même utilisateur ou l'association de ces sessions à un compte spécifique d'un utilisateur. Ces identifiants peuvent avoir une durée de vie courte, permettant de fragmenter les longues sessions (*I1*).
    - Identifiant pseudonyme propre à chaque utilisateur mais ne permettant pas directement d'identifier l'utilisateur correspondant. Un tel identifiant peut être créé en se reposant par exemple sur des fonctions de hachage (*I2*).
    - Identifiant limité à un domaine pour limiter la capacité à faire correspondre les sessions d'un même utilisateur sur plusieurs domaines (*I3*)

7.2 Assurer le respect du principe de limitation de la durée de conservation

45. Les données doivent être conservées pendant **une durée n'excédant pas celle nécessaire au regard des finalités poursuivies (article 5.1.e du RGPD).**

46. Le fournisseur de la solution devrait donc permettre à l'éditeur de configurer des durées de conservation et des règles de suppression en fonction des finalités poursuivies.

47. La CNIL recommande au fournisseur de mettre en œuvre une architecture technique permettant la possibilité de suppression de sessions individuelles, notamment pour répondre aux cas où la durée de conservation serait dépendante d'actions utilisateurs (suppression de la session suite à la clôture d'une demande de support par exemple) et en tout état de cause pour respecter les demandes de suppression des données. La CNIL recommande, dans le tableau ci-après, des durées de conservation en fonctions des finalités poursuivies.

7.3 Assurer le respect du principe de sécurité du traitement

48. L'éditeur et ses sous-traitants doivent mettre en œuvre **les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (article 32 du RGPD).** Dans le contexte des outils de rejeu de session, la CNIL recommande que l'éditeur puisse avoir à sa disposition les fonctionnalités suivantes :

- Blocage de la collecte de tout mot de passe, information bancaire, ou autre donnée soumise à des conditions particulières de collecte et de stockage en raison de leur sensibilité et des risques associés à une utilisation malveillante (*S1*).
- Outil permettant la mise en œuvre en œuvre d'une politique d'habilitation (avec des profils / rôles / droits distincts en fonction des données concernée) et la vérification de leur pertinence dans le temps comme toute mesure interne (revue périodique, mise à jour en cas de départ/mobilités internes) (*S2*).

Dans la mise en œuvre de l'ensemble de ces fonctionnalités, il est recommandé que le fournisseur propose toujours le paramétrage par défaut le plus protecteur possible, au titre de « La protection des données par défaut » (article 25 du RGPD).

8. Annexe 1

Explication : *le but de ce tableau est de permettre aux éditeurs d'identifier, finalité par finalité, les mesures techniques qu'il est recommandé d'appliquer (et partant, aux fournisseurs de proposer). A chaque finalité, couverte par la recommandation, correspond une série de mesures d'application cumulative ou alternative (dont le descriptif figure ci-dessous) permettant une utilisation des outils conforme à la règlementation.*

Finalité poursuivie	Besoin métier	Mesure de limitation des risques	Commentaire
Support et assistance pour gérer les demandes client (ou problème avec les services proposés)	Nécessité de pouvoir identifier la session associée à un identifiant spécifique (communiqué par le client ou associé à son compte) pour l'utiliser dans le cadre du support.	-L2 et (M3 ou M2 ou M1) et (I2 ou I3) et S1 et S2 -durée de conservation limitée à quelques heures après la fin de la session.	-Validation du démasquage : la situation d'exploitation se faisant suite à un contact avec l'utilisateur, la CNIL recommande d'avoir un processus de validation avec l'utilisateur préalable à tout démasquage. -La durée de conservation devrait être justifiée de manière documentée concernant l'occurrence dans le temps des situations de support.
Amélioration de l'expérience utilisateur (« UX »)	Identification de zones de frictions (rage clics, faux clics, etc.) afin de fluidifier la navigation et corriger d'éventuelles difficultés d'UX. La visualisation de session(s) individuelle(s) de navigation permet de compléter les données d'analyse agrégées car elle révèle des comportements non détectables au moyen de métriques d'analyse classiques. Nécessite un volume de données et une profondeur historique importante.	-(L1 ou L3) et (M2 ou M3) et I1 et S1 et S2 -durée de conservation de quelques mois afin de se limiter aux problématiques sur la version actuelle du site.	-La finalité poursuivie ne nécessite pas, d'association d'une session à un identifiant utilisateur. -Le démasquage ne peut être que très marginalement utile ce qui explique un procédé plus complexe.
Détection et compréhension des erreurs ou problèmes technique	Identification des erreurs, permet de comprendre le contexte y amenant à partir d'éléments de navigation obtenus en situation réelle et non détectables au moyen de métriques d'analyse classiques. Nécessite un volume significatif et une profondeur historique moyenne, mais sur une typologie particulière de situation (occurrence d'une erreur).	-(L2 ou L3) et (M1 ou M2 ou M3) et I1 et S1 et S2 -durée de conservation de quelques mois afin de se limiter aux problématiques sur la version actuelle du site.	-Pour cette finalité, il n'y a pas de justification à l'association d'une session à un identifiant utilisateur. -Le démasquage peut servir de manière ponctuelle pour identifier des problématiques provoquées par une entrée utilisateur spécifique.