Réponse à consultation
Passerelle de filtrage web

Association PURR

28 septembre 2025

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 consultation publique de la CNIL sur son projet de recommandation visant le déploiement d'une solution de filtrage web.

Table des matières

1. Sur la pertinence du projet de recommandation

Le projet de recommandation se contente, en substance, d'affirmer que les principes du RGPD s'appliquent aux passerelles de filtrage web, et de les décliner, sans plus de véritables précisions, ni juridiques ni techniques.

Ainsi, nous ne parvenons pas à mesurer l'apport de cette recommandation insipide et sans ambition. Il est regrettable et dommageable de voir la CNIL gaspiller ses moyens dans les lignes directrices se résumant à paraphraser le RGPD et n'apportant en pratique rien de fondamentalement nouveau par rapport au texte législatif, ce d'autant plus sachant la nécessité de lignes directrices sur d'autres sujets qui seraient réellement utiles et intéressantes pour encadrer des traitements aujourd'hui mis en œuvre de manière illicite.

Nous ne nous y opposons pas, mais nous déplorons que la recommandation ne soit pas plus fouillée, ainsi que le temps gaspillé par la CNIL pour la rédiger au détriment d'autres travaux.

2. Sur la forme

Afin d'augmenter la praticité du document, préciser, dès la page de garde, qu'il porte uniquement sur un accès à Internet dans le cadre professionnel.

3. Sur la rétention des données de connexion

Dans ses sections 1, sur la portée de la recommandation, et 4, sur les bases légales du traitement, le projet de recommandation pointe vers l'obligation légale de rétention des données de connexion (décrets 2021-1361, 2021-1362, et **2024-901** – le décret 2021-1363 pointé par la CNIL a expiré).

D'abord, nous rappelons que la directive européenne 2006/24/CE a été invalidée par la Cour de justice de l'UE en 2014[1]. Le décret français 2006-358 n'est plus d'actualité. L'obligation ajoutée dans la loi 86-1067 par la loi 2000-719 a été déplacée dans l'article 6 de la Loi pour la confiance dans l'économie numérique. L'article 32-3-1 du Code des postes et des communications électroniques (CPCE), ajouté par la Loi sur la sécurité quotidienne, est devenu le L34-1 du même code.

[1] Arrêt C-293/12

Nous demandons à la CNIL de retirer ces références obsolètes de la recommandation finale.

Ensuite, la recommandation porte sur l'accès à Internet dans un cadre professionnel. Ces acteurs n'étant ni des hébergeurs informatiques de contenus publics, ni des opérateurs de communications électroniques ouverts au public, l'obligation légale précitée ne leur est pas opposable[2], comme le consigne la documentation de la CNIL sur le sujet[3] : « *Les entreprises et les administrations fournissant un accès Internet, y compris par wi-fi, à leurs employés ne sont pas concernées par cette obligation de conservation. […] Si l'employeur propose aux visiteurs dans ses locaux un accès au réseau Internet par wi-fi, il est alors tenu de respecter les obligations applicables décrites sur cette page.* ».

De plus, la journalisation des connexions web (HTTP) est insuffisante pour satisfaire l'obligation qui porte sur l'ensemble des connexions et des protocoles.

À l'inverse, le filtrage et la journalisation du contenu, y compris de la seule URL, y compris du seul nom de domaine, dépassent l'obligation précitée. Pourtant, les dispositifs de filtrage web ont tendance à journaliser cela, comme le consigne la section 7 du projet de recommandation. Dès lors, ils ne sauraient reposer sur l'obligation de rétention des données de connexion.

Enfin, le Conseil d'État a interprété que ladite rétention porte uniquement sur ce qui est collecté ou traité dans le cadre normal de l'activité de l'entité qui y est soumise[4]. Or, à nouveau, les passerelles de filtrage web vont au-delà, afin de détecter des compromissions ou des violations de DCP. Dès lors, ils ne sauraient relever de l'obligation de rétention des données de connexion.

Ainsi, afin de sécuriser les acteurs et d'éviter tout traitement préjudiciable aux Personnes Concernées, nous demandons à la CNIL de cesser de fonder l'usage des passerelle de filtrage web sur l'obligation de rétention des données de connexion ou, a minima, de préciser et d'expliciter les cas et les conditions rappelées supra dans lesquels l'obligation légale précitée peut servir de base légale aux dispositifs de filtrage web (Wi-Fi visiteurs uniquement, pas de journalisation du contenu, y compris des noms

2. Délibération CNIL 2011-203
3. https://www.cnil.fr/fr/fournir-un-acces-internet-public-quelles-obligations
4. Décision CE 459724, point 9

de domaine, pas de filtrage, pas de conservation au-delà des seules DCP strictement nécessaires à la fourniture d'un point d'accès Wi-Fi visiteurs, etc.).

4. Sur la durée de conservation

La section 8 du projet de recommandation expose qu'une durée de conservation au-delà d'un an doit être justifiée et documentée.

Cette durée d'un an nous paraît très généreuse voire excessive au regard tant des types de DCP consignés, que des finalités poursuivies, que du caractère hautement intrusif qu'une telle journalisation constitue dans la vie privée des salariés ou agents.

En effet, il n'y a que peu sinon pas d'intérêt à vouloir rechercher une violation de DCP ou des indices de compromissions au-delà d'un an après la survenue de l'évènement. Un tel cas monterait plus une défaillance généralisée et un défaut de sécurisation rendant impossible la détection d'une compromission dans des délais raisonnables, et même à ce qu'une meilleure compréhension de l'attaque serait rendue possible par de tels logs très anciens, le risque pour les droits des Personnes Concernées ne justifie pas une telle conservation pour un intérêt très hypothétique.

Sur le caractère hautement intrusif, par analogie, l'obligation de rétention des données de connexion ne porte pas sur les domaines Internet ni sur le comportement des utilisateurs[5], elle est difficilement justifiée par une menace grave contre la sécurité nationale[6], et la conformité à la jurisprudence de la CJUE d'une telle durée de conservation est l'objet de débats doctrinaux animés[7].

La journalisation des accès au système d'information et des manipulations sur les DCP n'a que peu à voir avec celle des dispositifs de filtrage web. Ainsi, la recommandation sur la journalisation[8] n'est pas topique. D'ailleurs, les points deux à trois de ladite recommandation excluent les dispositifs de filtrage web de son champ d'application.

Dès lors, nous ne pouvons pas accepter une conservation dépassant quelques mois.

---

5. Article R10-13 du Code des postes et des communications électroniques
6. Décret 2024-901
7. Dans ses différents arrêts, notamment C-203/15, la CJUE s'oppose à une longue durée de conservation pour des finalités frivoles, y compris la criminalité grave
8. https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation_-_journalisation.pdf

Ainsi, afin de dissuader une telle démarche, nous demandons à la CNIL de consigner, dans la recommandation finale, qu'une durée de conservation supérieure à six mois doit être justifiée et documentée et qu'elle pourrait apparaître comme excessive.

5. Sur la conciliation avec l'usage personnel

De jurisprudence constante, la Cour de cassation admet que les salariés ont le droit, sur leur temps de travail, de faire un usage personnel du matériel mis à leur disposition, tant que cet usage est raisonnable.

La CNIL rappelle cela en filigrane en pointant l'article L1121-1 du Code du travail ou lorsqu'elle préconise que des catégories de sites web devraient être exclues du déchiffrement HTTPS.

La base légale préconisée étant l'intérêt légitime, qui nécessite tant un intérêt impérieux du Responsable de Traitement qu'un équilibre avec les droits des Personnes Concernées, nous demandons à la CNIL d'affirmer explicitement la conciliation entre les finalités du Responsable de Traitement et la vie privée et l'usage personnel des salariés ou agents.

Le projet de recommandation ne distingue pas un filtrage web opéré par le réseau de la société commerciale ou de l'administration, d'un filtrage opéré par un programme informatique, nommé agent, déployé sur le matériel mis à disposition des salariés ou agents (ordinateur portable, ordiphone, etc).

Pourtant, il sera rappelé que plusieurs produits de sécurité procèdent à une interception et au déchiffrement de l'ensemble des connexions réseaux, et que la presse a fait état de logiciels de prévention de la perte de données (Data Loss Prevention) utilisés abusivement (surveillance en dehors des heures travaillées, analyse de l'ensemble des flux et des activités, signalement d'emails comportant la mention « personnel », etc.)[9].

Or, un salarié ou un agent ne saurait faire l'objet d'un filtrage web et encore moins d'une journalisation de ses consultations web, en dehors de ses heures de travail, tant en télétravail que durant ses heures de pause dans le local de l'employeur.

Ainsi, nous demander à la CNIL de compléter sa recommandation en consignant qu'un débrayage de la journalisation et/ou du déchiffrement HTTPS et/ou une atténuation

[9] Exemple : https://www.lecanardenchaine.fr/social/6299-tata-yoyote-sur-la-protection-de-ses-donnees

du filtrage web devrait être mis en œuvre en fonction des heures travaillées ou sur action du salarié ou agent (une telle opération serait journalisée). À défaut, des ordinateurs en libre-service (avec identification si besoin) pourraient être mis à la disposition des salariés ou des agents sur leurs temps de pause.

De même, nous demandons à la CNIL de retirer le fragment de phrase « *(besoin d'ajout d'une URL spécifique nécessaire à l'exercice de ses fonctions)* » de la section 7. En effet, toute URL pertinente pour un usage personnel (journal, santé, réseaux sociaux, etc.) devrait pouvoir être exclue du déchiffrement HTTPS sur demande d'un salarié, d'un agent, ou d'un représentant du personnel œuvrant comme intermédiaire (afin de préserver la vie privée).

De même, les catégories de sites exclus du déchiffrement HTTPS ne sauraient être restreintes à « *(banques, santé, administrations publiques, etc.)* ». Nous demandons à la CNIL de préciser qu'il s'agit là d'exemples. Tout site web pertinent pour un usage personnel, notamment celui destiné à recevoir ou afficher des DCP, devrait être exclu du déchiffrement HTTPS.

De même, nous demandons à la CNIL d'ajouter que les pages d'identification (saisie d'un identifiant et d'un mot de passe) de tout site web devraient être exclues du déchiffrement HTTPS. Il en va de même des pages dont il est prévisible qu'elles affichent des DCP (« mon compte », « espace personnel », « espace client », etc.).

De même, nous demandons à la CNIL de consigner que la présence ou l'absence de déchiffrement HTTPS et/ou de journalisation devrait être modulée en fonction du type de terminal : le trafic Internet du réseau des serveurs informatiques pourrait être plus lourdement bridé et surveillé que celui regroupant des postes informatiques dédiés à des usages précis et ponctuels dans une journée de travail, que celui regroupant les postes de travail usuels pour le tout-venant.

Pour l'association PURR

[redacted] [redacted]

Membre du Conseil Membre du Conseil

[redacted] [redacted]