Consultation publique sur le projet de recommandation relative aux mesures de journalisation

Synthèse des contributions

Le 28 mai 2021, la CNIL a lancé une consultation publique sur son projet de recommandation relative aux mesures de journalisation afin de recueillir les difficultés d'interprétation suscitées par le texte. Les contributions ont nourri les travaux de la CNIL en vue de la publication de la *recommandation*.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Synthèse des contributions de la consultation publique sur le projet de recommandation relative aux mesures de journalisation

Cette consultation publique a fait l'objet de contributions, principalement de professionnels du secteur (DPD/DPO et RSSI), concernés par les travaux de la CNIL sur le sujet de la journalisation. La CNIL propose ici une synthèse des contributions.

À propos de la consultation publique de la CNIL sur son projet de recommandation relative aux mesures de journalisation

Les systèmes de journalisation sont des outils indispensables pour la sécurité des données à caractère personnel, qui peuvent notamment permettre de détecter des incidents ou des accès non autorisés. Afin d'aider les responsables de traitement à mettre en place des mesures adaptées, la CNIL a élaboré un projet de recommandation précisant les mesures à mettre en place en fonction des caractéristiques du traitement principal, notamment en termes de durée pendant laquelle les données de journalisation doivent être conservées.

Ce projet a fait l'objet d'une consultation publique entre le 28 mai et le 25 juillet 2021, en vue de la préparation de la version définitive de la recommandation.

Quelques chiffres

La consultation a reçu 43 commentaires de la part de 26 participants :

- **84% de ces participants ont jugé que le périmètre de la recommandation était pertinent** ;
- **15 sont des délégués à la protection des données (DPD/DPO)** ou RSSI ;
- **3 sont des particuliers ;**
- les 8 derniers ont des profils variés (juriste du secteur, ingénieur informaticien ou manager).

Ces contributions ont permis à la CNIL :

- de faire évoluer, sur le fond et sur la forme, le projet de recommandation afin d'y apporter certaines clarifications. Ces clarifications concernent :
  - un paragraphe rappelant les risques liés aux détournements de finalité des données ;
  - un exemple sur les modalités d'information aux utilisateurs habilités ;
  - un paragraphe explicitant les modalités à prévoir en cas de recours à la sous-traitance ;
  - un paragraphe explicitant auprès de qui doit s'effectuer l'exercice des droits, ainsi que les modalités d'inscription au registre ;
  - des reformulations visant à éviter des confusions en termes de textes applicables pour les parties « Cas des contrôles internes » et « Autres cas » ;
  - une précision sur l'origine juridique de la notion de « données sensibles » ;
  - des reformulations mineures sur des éléments qui provoquaient des incompréhensions ;
- d'apporter des réponses, dans la synthèse ci-dessous, aux préoccupations et incompréhensions exprimées, particulièrement lorsqu'elles n'avaient pas vocation à faire évoluer la recommandation.

La suite de ce document présente les réponses aux interrogations les plus courantes.

Sur la question de l'interaction de la recommandation avec les principes du RGPD

De nombreuses questions sont posées sur **l'application des différents principes du RGPD à la journalisation**. De manière générale il convient de noter que **dans le cas où la journalisation est adossée à un traitement qui relève du RGPD, les principes de celui-ci s'appliquent à la journalisation.**

Les modalités de gestion dans le cas du recours à la sous-traitance

Certains participants demandent plus de précisions en ce qui concerne les modalités de gestion dans le cas du recourt à la sous-traitance, notamment dans le cas de l'utilisation d'un service en mode « SaaS » (pour « *Software as a Service* » – logiciel hébergé dans l'informatique en nuage).

« Il pourrait être utile de préciser le rôle des sous-traitants dans la mise en place de dispositifs de journalisation (obligation propre de sécurité incombant aux ST conformément à l'art. 32 du RGPD ?) »

« Il serait intéressant de recommander au RT, l'introduction lors d'une conception d'outil ou un appel d'offre de solution logicielle traitant des DCP d'introduire la dimension de journalisation respectant la description faite au Point 6. »

En ce qui concerne le recours à des sous-traitants, les textes applicables précisent déjà la situation, notamment via les articles 32 et 28 du RGPD ou l'article 3 du titre III de la loi « Informatique et Libertés ». Il est important de préciser que, dans la mesure où le responsable de traitement définit les traitements qui sont opérés, c'est bien à lui de définir la journalisation à mettre en place. Ainsi, si un appel d'offres est émis par un responsable de traitement, il est important qu'il intègre dans celui-ci les éléments nécessaires pour la bonne mise en œuvre de la présente recommandation, charge au sous-traitant de lui permettre d'atteindre cet objectif. Cela signifie également que dans le cas de l'utilisation d'un service SaaS, le sous-traitant fournissant l'outil logiciel doit fournir une interface permettant ou responsable de traitement de répondre à ses obligations. Un paragraphe a été ajouté dans la recommandation pour préciser ce point.

La prise en compte des droits des personnes visés

Des questions ont été soulevées sur ce sujet, que ce soit en termes d'information ou d'exercice des droits à proprement parler.

« Il manque votre position sur l'exercice des droits des personnes concernées pour la journalisation. […]»

« La mention d'information est spécifique (souvent portée sur la page d'authentification des utilisateurs et/ou dans des CGU de lecture obligatoire […] »

En ce qui concerne les respects des droits des personnes, rien ne permet d'écarter de manière générale la possibilité pour elles d'exercer leurs droits sur les données de journalisation. Les textes applicables listent chacun de ces droits et précisent les contextes dans lesquelles ils peuvent s'exercer. C'est donc une analyse à effectuer au cas par cas. Pour clarifier ce point, un paragraphe est ajouté afin d'expliciter que l'exercice des droits s'effectue auprès du responsable du traitement auquel la journalisation est appliquée. En ce qui concerne l'information des utilisateurs, c'est à la fois une mesure qui relève des textes et qui participe également, dans certains contextes, à la finalité de sécurisation du traitement ; c'est la raison pour laquelle ce point est rappelé au paragraphe 13. Ce point est précisé pour donner un exemple de mise en œuvre.

La nécessité de l'inscription au registre du traitement de journalisation

Certains participants posent la question de l'applicabilité de l'obligation de la tenue du registre aux opérations de journalisation.

« Il est fastidieux de documenter dans le registre des traitements que, lors d'un traitement concernant les usagers, les données des agents en charge de ce traitement sont collectées au travers des journaux. […] »

« Faut-il prévoir un traitement spécifique à la journalisation dans le registre ? »

En ce qui concerne l'inscription au registre, encore une fois rien ne permet d'écarter de manière générale cette inscription, qui est obligatoire si le traitement et le responsable de traitement remplissent les critères qui le justifient. Cette inscription de la journalisation adossée à un traitement peut être réalisée de manière alternative au sein de l'entrée du registre relative au traitement auquel la journalisation est adossée la journalisation, ou bien dans une entrée spécifique du registre dans le cas d'une journalisation transversale et commune à différentes opérations de traitement. Ce point est donc précisé dans la recommandation. Dans le cas d'un traitement dont la finalité principale serait la journalisation elle-même, cette inscription devrait alors se faire de manière indépendante, mais ce n'est pas le contexte évoqué dans la présente recommandation. On peut relever à cet égard que la pratique des ministères en matière de formalités est conforme à ces principes : les systèmes de journalisation mis en place dans le cadre de traitements spécifiques sont encadrés par l'acte réglementaire encadrant le traitement, tandis que les systèmes de journalisation indépendants font l'objet de saisines spécifiques.

La nécessité de réaliser une AIPD

« Une AIPD de manière générale est-elle requise ? »

Sur la nécessité ou non de réaliser une AIPD, il est tout d'abord important de noter que l'AIPD est un outil utile pour analyser les risques associés au traitement. Dans le contexte de la journalisation, il peut notamment permettre de déterminer si une durée de conservation plus longue que la recommandation générique peut se justifier au regard de risques spécifiques que d'autres mesures ne permettent pas de traiter. Cependant, **dans le cas général, elle n'est pas obligatoire. Les critères d'obligation restent ceux du RGPD, précisés par les lignes directrices du CEPD[1] et la délibération de la Commission portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise[2].**

La directivité générale des recommandations

Certains répondants demandent à la CNIL plus de directivité dans ses recommandations, notamment en termes de durée de conservation des données de journalisation, quant à la la notion de « risque excessif » du paragraphe 15, ou bien dans la qualification des situations qui peuvent permettre au responsable de traitement de justifier un allongement supplémentaire tel que décrit dans le paragraphe 17.

« J'aurais souhaité que cette recommandation soit prescriptive, afin d'éviter toute notion de subjectivité dans la lecture, l'analyse et la compréhension de la recommandation et dans la détermination des durées de conservation. »

« Comment qualifier un risque « excessif » ? »

Encore une fois, le principe directeur est tiré du RGPD, celui de la redevabilité (« *accountability* »). Si la CNIL peut présenter les critères qui permettent d'analyser la situation, **la diversité des traitements rend indispensable que chaque responsable de traitement réalise une analyse spécifique de sa situation pour déterminer les mesures proportionnées à mettre en œuvre.** Néanmoins, dans un souci de clarté, la CNIL a indiqué une durée recommandée de six mois à un an pour les journaux, qui constitue un point de référence pour les responsables de traitement ne souhaitant pas conduire d'analyse au cas par cas.

[1] https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf
[2] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039248939

Autres sujets abordés dans les réponses à la consultation publique

Un participant à la consultation pose la question des régimes juridiques applicables à chacune des parties de la recommandation.

« SUR LE §13 – […] s'interroge sur le titre donné à cette partie qui semble concerner certains traitements et en particulier les traitements relevant de la directive dite « police-justice »

« SUR LE §17 – La Commission devrait préciser de façon explicite que les traitements présentant des spécificités pouvant justifier un allongement supplémentaire de la durée de conservation vise[nt] tout traitement […] »

Les traitements visés par ces recommandations sont explicités par le paragraphe 4, c'est-à-dire les traitements de données à caractère personnel soumis à des obligations « en application des articles 5 et 32 du RGPD, ainsi que des articles 99 et 101 de la loi « Informatique et Libertés » pour les traitements soumis à la directive « Police-Justice » et, pour les traitements soumis à la seule loi « Informatique et libertés », de l'article 121 de cette loi ». Le texte proposé à la consultation pouvait effectivement porter à confusion, notamment concernant son paragraphe 13. Celui-ci a donc été modifié pour clarifier le fait qu'aucune partie de la recommandation n'était limitée à une sous-partie des traitements déclarés au paragraphe 4.

Un participant à la consultation pose la question de l'applicabilité de la recommandation à des SIEM.

« Ce guide ne semble pas s'appliquer aux outils comme le SIEM qui se connecte à un système pour collecter, analyser les données. »

Les SIEM (pour « *security information and event management* » – système de gestion des événements et de la sécurité) sont des outils regroupant des fonctionnalités de collecte, de croisement, de valorisation, de *reporting*, de rejeu et d'archivage. Leurs fonctionnalités sont bien visées par la présente recommandation, notamment en son paragraphe 9, qui vise les fonctionnalités d'analyse à mettre en place. Pour le reste, ces systèmes sont soumis aux mêmes recommandations que les autres types d'outils de gestion des traces.

Un participant pose une question relative aux difficultés techniques à mettre en œuvre certaines recommandation, notamment celle lié à la séparation physique des infrastructures.

« Séparer physiquement les logs de l'applicatif est très coûteux. »

Les recommandations et, notamment, les recommandations techniques, sont évidemment à appliquer en fonction des caractéristiques du traitement et des capacités techniques du responsable de traitement. Il est donc tout à fait possible qu'une structure n'ait ni la nécessité (en termes de sécurisation du traitement) ni la capacité à mettre en œuvre une des mesures proposées.

Un participant pose la question de savoir si cette recommandation abroge et remplace la recommandation de conserver les données de journalisation pendant six mois présente dans le guide sécurité**.**

« Cette nouvelle recommandation vient-elle amender les recommandations existantes ? »

Effectivement, les contenus mis à disposition par la CNIL seront mis à jour pour intégrer cette modification de la doctrine.

Un participant nous demande de souligner l'aspect problématique de la réutilisation des données collectées dans le cadre de la journalisation.

« Le risque principal est un risque de réutilisation des journaux de connexion pour d'autres finalités que le suivi technique et la sécurité. Par exemple, les journaux d'ouverture et de fermeture de session d'un poste de travail pourraient être utilisés pour mesurer la durée du travail d'un employé. […] »

Effectivement, une réutilisation des données à des fins autres que ce qui est présenté dans la journalisation constitue un détournement de finalité. Bien que le sujet soit évoqué au paragraphe 5, il a été décidé d'ajouter un paragraphe 9bis pour préciser ce point.

Un participant demande de préciser comment il est possible de faire référence aux données visée par l'opération journalisée sans pour autant copier cette donnée dans les journaux.

« S'agissant de la référence des données concernées par l'opération : la CNIL pourrait utilement préciser comment mettre en œuvre celle-ci sans pour autant procéder à la duplication des données ? »

Le paragraphe 19 explicite la manière dont il est possible de stocker dans des journaux, non pas la donnée visée par la journalisation en elle-même mais un identifiant y faisant référence, la table de correspondance devant dès lors être stockée avec la donnée afin de s'assurer que la suppression de la donnée source rende toute réidentification particulièrement difficile.

La version amendée de la recommandation, adoptée le XXX, est disponible ICI.

Document de référence

- La loi « Informatique et Libertés »
- Le RGPD
- La recommandation relative aux mesures de journalisation
- Le site web de la CNIL