PROJET DE RECOMMANDATION

relative à la journalisation

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

29 avril 2021

1. La présente délibération constitue une recommandation relative aux modalités de conservation et d'usage des données de journalisation. Elle vise à harmoniser les pratiques des différents responsables de traitement, et tient compte d'échanges avec des parties prenantes et du résultat de la consultation organisée sur ce sujet.

2. Cette recommandation a pour champ d'application la mise en œuvre de dispositifs de journalisation. L'analyse et les recommandations exprimées dans cette recommandation sont indépendantes de la nature du responsable de traitement, qui peut être un organisme public ou privé, et ne s'appliquent pas aux traitements dont la finalité principale serait la journalisation elle-même.

3. Les dispositifs de journalisation sont définis comme les dispositifs qui permettent d'assurer une traçabilité des accès et des actions des différents utilisateurs habilités à accéder aux systèmes d'information et, partant, aux traitements de données à caractère personnel mis en œuvre au sein de ces systèmes. Ces dispositifs peuvent être adossés soit à des applications (qui sont les briques logicielles spécifiques au traitement mis en œuvre et sont donc sujettes à la mise en œuvre de journaux dits « applicatifs »), soit à des équipements spécifiques (qui sont des équipements informatiques associés à des logiciels embarqués, sujets à la mise en œuvre de journaux dits « périmétriques »). La présente recommandation est applicable aux dispositifs de journalisation liés à l'application sur laquelle repose le traitement et non à la journalisation périmétrique.

4. La mise en place d'un dispositif de journalisation participe au respect de l'obligation de sécurisation de tout traitement de données à caractère personnel, en application de l'article 5 et de l'article 32 du RGPD, pour les traitements soumis à la directive « Police-Justice » des articles 99 et 101 de la loi « informatique et libertés » et, pour les traitements soumis à la seule loi « informatique et libertés », de l'article 121 de cette loi. Ces dispositifs peuvent, dans certains cas, poursuivre d'autres finalités (voir ci-dessous, section « Autres cas »). Ils peuvent notamment permettre de documenter les transmissions de données à des « destinataires », afin de satisfaire à l'obligation pour le responsable de traitement d'être en capacité de fournir aux personnes concernées une information sur les « destinataires ou catégories de destinataires auxquels les données le concernant ont été communiquées » et sur les informations qui leur ont été communiquées (art. 15 du RGPD ; voir CJUE, 7 mai 2009, Rijkeboer, C-553/07, Rec.). La durée de conservation des journaux doit alors tenir compte de cette finalité spécifique, dans le respect de la jurisprudence de la CJUE. La CNIL souligne que cette obligation du responsable de traitement peut également être satisfaite par d'autres moyens que les dispositifs de journalisation.

5. A cet égard, il est nécessaire de trouver un équilibre entre la sécurité apportée par la journalisation, la surveillance que ce type de système peut créer pour les utilisateurs habilités et l'émergence de risques particuliers liés à une conservation trop longue. Dans la majorité des cas, les données journalisées contiennent des données relatives aux personnes concernées par le traitement principal. En conséquence, l'enregistrement de ces données de journalisation ne modifie pas la sensibilité de ces traitements, mais peut offrir des garanties importantes pour la sécurité de ces données. En revanche, ces journaux contiennent également des données relatives aux utilisateurs habilités du système. Ces données peuvent révéler des informations sur ces individus, notamment des informations relatives à leur comportement professionnel. Il convient de veiller à limiter les risques portant sur ces catégories de personnes, en proportionnant la collecte, au sein des journaux, de données à caractère personnel relatives aux utilisateurs habilités, à la sensibilité des données à caractère personnel du traitement principal et aux risques qu'un mésusage de celui-ci ferait courir aux

personnes concernées. La présente délibération présente les recommandations de la CNIL pour trouver cet équilibre en fonction de différents cas de figure.

Cas général

6. La Commission recommande que les opérations de création, consultation, modification et suppression des données à caractère personnel et des informations contenues dans les traitements auxquels la journalisation est appliquée fassent l'objet d'un enregistrement comprenant l'auteur individuellement identifié, l'horodatage, la nature de l'opération réalisée ainsi que la référence des données concernées par l'opération. Il convient notamment d'éviter de dupliquer au sein des journaux les données concernées par le traitement. Cette journalisation peut être intégrée au niveau applicatif ou bien gérée au niveau technique au moyen des ressources logicielles utilisées par l'application.

7. La Commission recommande de conserver ces données de manière ségrégée du système principal, par exemple sur des équipements physiquement distincts et accessibles uniquement en écriture par les applicatifs du traitement principal, sans possibilité d'écrasement de données existantes. L'attribution des droits d'accès aux données de journalisation doit faire l'objet d'autorisations spécifiques basées sur la stricte nécessité.

8. La Commission recommande de conserver ces données pendant une durée comprise entre six mois et un an. Elle estime en effet que cette durée est suffisante, dans la plupart des cas, afin d'assurer un équilibre entre, d'une part, la nécessité de disposer de données de journalisation permettant d'identifier les atteintes au système de traitement et, d'autre part, la nécessité de ne pas conserver un volume de données trop important pouvant faire l'objet d'attaques ou de détournements de finalité.

9. La conservation de ces données de traçabilité est justifiée par l'objectif de sécurisation du traitement. Cette sécurisation est essentiellement « active » : elle repose sur une exploitation en temps réel ou à court terme de ces données pour détecter des opérations anormales afin de parer des attaques ou intrusions ou de remédier rapidement à un incident informatique en facilitant l'identification du problème. La Commission recommande dès lors de mettre en œuvre un système de traitement et d'analyse des données collectées et de formaliser un processus permettant de générer des alertes et de les traiter en cas de suspicion de comportement anormal.

10. Ces données peuvent également servir *ex post* lorsqu'une violation de données (notamment par consultation, transmission ou usage illégaux des données) est constatée et que le responsable de traitement cherche à en établir la responsabilité.

11. L'existence de journaux recopiant certaines des données contenues dans le fichier conduit, lorsque ces données sont sur le point d'être supprimées du fichier, à les conserver plus longtemps que leur durée de conservation initiale. Si ce phénomène est souvent inévitable et acceptable eu égard au rôle que jouent ces dispositifs de journalisation dans la sécurité du traitement, la Commission recommande d'essayer de limiter au maximum cette extension de la durée de conservation. La conservation des données de traçabilité ne doit pas conduire les responsables de traitement à conserver de manière excessive des données à caractère personnel au-delà de celles du traitement principal. Elle recommande également de minimiser l'inclusion de données à caractère personnel dans les données de journalisation.

En tout état de cause, le responsable de traitement doit définir des modalités permettant de garantir la confidentialité, la disponibilité et l'intégrité des données de journalisation. En particulier, la Commission recommande d'horodater et de signer les journaux dès leur création. De même, les modalités d'utilisation des traces collectées doivent faire l'objet de règles et de procédures formalisées et documentées.

12. Les utilisateurs habilités à accéder au traitement doivent être informés de la mise en place du dispositif de journalisation, de la nature des données collectées et de la durée de conservation de ces dernières.

Cas de contrôles internes

13. Pour certains traitements, en raison de l'importance du risque pour les personnes en cas de détournement des finalités du traitement et de la fréquence d'occurrence de telles pratiques, ou pour les traitements soumis aux articles 99 et 101 de la loi n° 78-17 du 6 janvier 1978, la Commission estime qu'une journalisation pour une durée supérieure à un an peut également contribuer au contrôle interne. La capacité dissuasive d'un tel processus participe alors à la sécurité du traitement en limitant les risques d'atteinte à la sécurité du traitement principal. Une durée supérieure à un an peut donc participer à constituer une garantie appropriée de la protection de la vie privée des personnes concernées au regard des risques spécifiques liés à ce type de traitement.

14. Pour justifier de son usage à cette fin, il est recommandé que le responsable de traitement :

- démontre le risque, pour les personnes concernées par le traitement principal, lié à un détournement de la finalité de l'utilisation des données les concernant. Ce point peut être notamment justifié par le fait que le traitement projeté ou mis en œuvre traite des données sensibles ou d'infraction, à grande échelle ou conduit à une surveillance systématique des personnes concernées ;
- dispose de procédures documentées en matière d'analyse et d'investigation internes, de manière régulière et en cas de signalement ou de suspicion de détournement de finalité.

15. La Commission rappelle que la mise en œuvre d'une telle politique de traçabilité ne doit pas en principe conduire le responsable de traitement à collecter des données présentant des risques excessifs d'atteinte à la vie privée pour les personnes accédant ou concernées par les journaux de connexion, notamment des données sensibles ou hautement personnelles, lorsque ces données ne sont pas déjà présentes dans le traitement.

16. Elle indique également que la durée de conservation des journaux devra dès lors être déterminée de manière proportionnée à la finalité poursuivie, notamment en fonction des temporalités décrites dans les processus du responsable de traitement. Le responsable de traitement devra également tenir compte de la durée de conservation des données du traitement pour déterminer une durée de conservation des traces proportionnée. Dans les cas les plus courants, une durée maximale de trois ans pourra ainsi être justifiée. En tout état de cause, la Commission rappelle qu'il n'est pas possible de motiver la durée de conservation des données de traçabilité par la seule durée de prescription des infractions pénales délictuelles liées au mésusage des données du traitement par ceux qui y accèdent.

Autres cas

17. Certains traitements présentent des spécificités qui peuvent justifier un allongement supplémentaire de la durée de conservation des données de journalisation. Elles peuvent, par exemple, correspondre :

- à une obligation légale de conserver des traces pour une durée précisée par les textes ;
- à une finalité spécifique atteinte à l'aide des données de journalisation, comme par exemple dans le cadre d'un traitement permettant la gestion des contentieux pour prouver que les parties ont bien accédé aux pièces et aux actes de procédure ou encore pour permettre une certaine transparence vis-à-vis des personnes concernées ;
- au besoin de pouvoir réaliser des analyses post-attaque ou post-intrusion, ou suite à une suspicion d'attaque liée à l'évolution de la connaissance de la menace dans un système de traitement automatisé de données.

18. Le responsable de traitement doit pouvoir justifier, de manière précise et documentée, des raisons le conduisant à envisager une durée plus longue, par exemple en excipant d'une obligation légale particulière ou de particularités liées à la finalité qui est poursuivie. La nécessité de conserver les données pendant une période plus longue peut également être justifiée par le fait que cette mesure constitue la seule manière de traiter des risques élevés pour les personnes dans le cadre d'une analyse d'impact relative à la protection des données (AIPD) ou d'une étude équivalente. Cette analyse doit être menée au cas par cas en appliquant les principes du RGPD, pour déterminer les garanties en termes de conditions de sécurité, d'accès et de finalités du stockage de ces données.

19. A l'inverse, lorsque la durée de conservation des données à caractère personnel du traitement principal est inférieure à six mois, il est nécessaire d'aménager les pratiques pour éviter une conservation des données du traitement dans les journaux au-delà de la durée prévue, tout en préservant l'intégrité des journaux. En pratique, pour ce type de cas, la Commission recommande de ne pas conserver dans les journaux des données à caractère personnel issues du traitement principal. Le journal peut ne conserver que des identifiants pseudonymes, ou pour lesquels la réidentification est particulièrement difficile. En cas d'impossibilité, il est aussi possible de mettre en place des procédures et outils de purge automatique des journaux visant à supprimer au sein de ceux-ci les données issues du traitement principal dont la durée de conservation est échue.

20. La présente recommandation concerne les mesures de journalisation applicables à des traitements génériques ; des mesures additionnelles de protection peuvent être nécessaires pour certains traitements. La conduite d'une AIPD est recommandée pour déterminer les mesures complémentaires adéquates.