Commission nationale de l'informatique et des libertés

Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation

NOR : CNIL2132269X

La Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD) ;

Vu la directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision cadre 2008/977/JAI du Conseil ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-I-2°-b), ci-après loi « informatique et libertés » ;

Après avoir entendu le rapport de M. François PELLEGRINI, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement ;

Adopte la présente recommandation :

La présente délibération constitue une recommandation relative aux modalités de conservation et d'usage des données de journalisation. Elle vise à faciliter la mise en conformité des différents responsables de traitement, et tient compte d'échanges avec des parties prenantes et du résultat de la consultation organisée sur ce sujet. Cette recommandation, et notamment les exemples qui y sont proposés, n'est ni prescriptive ni exhaustive et a pour seul objectif d'aider les professionnels concernés dans leur démarche de mise en conformité.

Les dispositifs de journalisation sont définis comme des dispositifs qui permettent d'assurer une traçabilité des accès et des actions des différents utilisateurs habilités à accéder aux systèmes d'information (et donc aux traitements de données à caractère personnel que sont susceptibles de constituer 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, qui répond à une logique différente.

Cette recommandation a pour champ d'application la mise en œuvre de dispositifs de journalisation. L'analyse et les recommandations contenues dans le présent document s'appliquent de la même manière à un organisme public ou privé, et ne s'appliquent pas aux traitements dont la finalité principale serait la journalisation elle-même.

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 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. 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 (voir notamment l'article 15 du RGPD et la décision de la Cour de justice de l'Union européenne (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 Commission souligne que cette obligation du responsable de traitement peut également être satisfaite par d'autres moyens que les dispositifs de journalisation.

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 personnes, 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 Commission pour trouver cet équilibre en fonction de différents cas de figure.

Cas général

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.

La Commission recommande de conserver ces données de manière ségréguée du système principal. Une modalité de mise en œuvre peut consister à utiliser 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 devrait faire l'objet d'autorisations spécifiques basées sur la stricte nécessité.

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, pour 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.

La conservation de ces données de traçabilité est d'abord 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.

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.

Toute réutilisation des données collectées pour des finalités autres que celle de la sécurisation du traitement est susceptible de constituer un détournement de finalité. Il convient donc que le responsable de traitement mette en œuvre les mesures techniques et organisationnelles permettant de limiter ce risque, par exemple par l'engagement des personnes accédant à ces données à respecter une charte d'utilisation définissant les usages acceptables de celles-ci, ou la levée d'une alerte spécifique en cas d'accès en modification aux données de journalisation par un compte habilité.

L'existence de journaux recopiant certaines des données contenues dans le fichier peut conduire, 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 de limiter au maximum cette extension de la durée de conservation. La conservation des données de traçabilité ne devrait 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 en principe faire l'objet de règles et de procédures formalisées et documentées.

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. Cela peut par exemple être réalisé *via* des mentions d'information présentées au moment de l'authentification lors de l'accès au traitement. Dans la mesure où les journaux sont accessoires à un traitement principal et dans un souci de clarté pour les responsables de traitement, la Commission recommande que les droits des personnes, tels que décrits au chapitre III du RGPD ou bien au chapitre III du titre III de la loi « informatique et libertés » relativement à la journalisation, s'exercent auprès du responsable du traitement principal.

La Commission recommande que, lorsque le traitement de données à caractère personnel devant faire l'objet d'une mesure de journalisation est mis en œuvre, en totalité ou en partie, par un sous-traitant au sens du RGPD et de la loi « informatique et libertés », le contrat de sous-traitance prévoit une obligation de journalisation conforme à la présente recommandation.

Concernant l'inscription au registre de traitements tel que prévu par l'article 30 du RGPD ou par l'article 100 de la loi « informatique et libertés », la Commission considère que celle-ci peut être réalisée de manière alternative au sein de l'entrée du registre relative au traitement auquel la journalisation est adossée, ou bien dans une entrée spécifique du registre dans le cas d'une journalisation transversale et commune à différentes opérations de traitement.

Cas de contrôles internes

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, la Commission estime qu'une journalisation telle que décrite au paragraphe 6 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.

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.

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 (telles que définies au paragraphe 1 de l'article 6 de la loi « informatique et libertés » et au paragraphe 1 de l'article 9 du RGPD) ou hautement personnelles, lorsque ces données ne sont pas déjà présentes dans le traitement.

Elle rappelle 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.

Autre cas

Certains traitements, quel que soit le régime juridique qui leur est applicable, 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 précise prévue 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.

Il est recommandé que le responsable de traitement justifie, 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 devrait être menée au cas par cas en appliquant les principes du RGPD, et de la loi « informatique et libertés » le cas échéant, pour déterminer les garanties nécessaires en termes de conditions de sécurité, d'accès et de finalités du stockage de ces données.

A l'inverse, lorsque la durée de conservation des données à caractère personnel du traitement principal est inférieure à six mois, il est préconisé 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 des identifiants 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.

Enfin, il est rappelé que, en application des lois en vigueur, les données des journaux de connexion peuvent faire l'objet d'une communication à certains « tiers autorisés », notamment dans le cadre d'enquêtes de police ou de procédures pénales à la suite d'une violation de données.

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.

La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
M.-L. DENIS