n°71
[Juillet - Août 2019]

www.village-justice.com

Le Journal du Management
juridique et réglementaire

legiteam Editions

LA PURGE DES DONNÉES PERSONNELLES : UN EFFORT QUI EN VAUT LA PEINE

Dès la première version de la loi Informatique et Libertés, en 1978, l'une des règles d'or concernant les données personnelles faisant l'objet d'un traitement obligeait le responsable de traitement à ne pas conserver ces informations dès lors que l'objectif visé était atteint. Le RGPD (Règlement Général de Protection des Données), entré en application le 25 mai 2018, a repris sans modification cette règle, comme en dispose son article 5.1.e : « *Les données à caractère personnel doivent être .../... conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées...* ». En d'autres termes, il est interdit de conserver des données personnelles sans limite, comme le précise le considérant 39 : « *Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum* ».

La CNIL veille à l'application de ce principe et vient ainsi de sanctionner à hauteur de 400.000 € la société SERGIC pour avoir insuffisamment protégé les données des utilisateurs de son site web et mis en œuvre des modalités inappropriées[1] de conservation des données. Par cette sanction, l'autorité de contrôle confirme l'achèvement de la transition vers le RGPD[2] : « *Il est essentiel que, désormais, les organismes appliquent complètement le nouveau texte. Dans l'instruction des plaintes et dans ses contrôles, la CNIL vérifiera donc pleinement le respect des nouvelles exigences. Elle en tirera au besoin toutes les conséquences, y compris en termes de sanction* ».

Comme toutes les autres règles relatives aux données personnelles, son respect pèse sur le responsable de traitement (le PDG, le Maire, le Président d'un Conseil départemental, le responsable d'un établissement de soins, etc.). Cette règle, vieille de quarante et un ans, est pourtant rarement respectée intégralement sur le terrain, pour plusieurs raisons : l'absence (jusqu'à ces derniers jours) de sanction, la crainte de se séparer

Bruno Rasle

d'une donnée... et d'en avoir besoin le lendemain (le syndrome du « On ne sait jamais... »), le fait que le stockage informatique coûte de moins en moins cher, l'absence de prise en compte de ce sujet lors de la conception des applications.

Mais une nouveauté introduite par le RGPD change totalement la donne : l'obligation de notifier les violations de données (à la CNIL et, dans certains cas, aux personnes concernées). En effet, pourquoi prendre le risque de devoir informer l'autorité de contrôle d'un manque de sécurité à l'occasion d'un incident survenu sur des données... qui auraient dues être purgées depuis longtemps ? N'est-ce pas là un bel exemple de masochisme ? L'observation rigoureuse des durées de conservation correspond à une réduction de la surface d'exposition, donc à une réduction du risque (pour les personnes, mais aussi pour l'entreprise). D'ailleurs il est intéressant de noter que les entreprises américaines – qui elles ont pourtant la possibilité légale de conserver les données sans limite – veillent à purger la moindre information qui ne leur rapporte plus un dollar : pourquoi continuer à stocker, indexer, sécuriser, sauvegarder une donnée dont on ne plus tirer aucune valeur ?

Et c'est souvent lors de la gestion d'une demande de droit d'accès exercé par une personne concernée au titre de l'article 15 du RGPD que cette non-conformité saute au visage : que faire en effet quand on découvre que l'on détient encore des données qui auraient dues être purgées depuis longtemps ? Ainsi, l'un des étudiants du Mastère Spécialisé « Informatique et Libertés » de l'ISEP, dans le cadre d'un projet piloté par l'auteur de ces lignes, a eu la surprise de recevoir de la part d'une chaîne de cinéma la liste très détaillée de tous les films qu'il avait été voir ces vingt dernières années (avec l'indication de la salle et de l'heure de la séance). Lui-même avouait ne plus se souvenir de certains de ces films. Quelle finalité peut justifier une telle durée de conservation ?

Mais qui détermine la durée de conservation ? Si l'obligation légale pèse bien sur le représentant de la personne morale, on voit mal le dirigeant préciser, traitement par traitement, combien de temps les données personnelles doivent être maintenues. Trop souvent, cette responsabilité est laissée aux bons soins de la MOE (la DSI ou le sous-traitant à qui a été confié le développement), voir au DPO (*Data Protection Officer*). C'est une erreur. La durée de conservation étant intimement liée à la finalité poursuivie, c'est à la MOA Métier de l'objectiver. Elle est la mieux placée pour – après avoir clairement exprimé l'objectif poursuivi – déterminer la durée indispensable à l'atteinte de celui-ci. De plus, la MOA doit justifier cette durée, pour respecter l'obligation d'*Accountability* imposée par le RGPD (en clair, il ne suffit pas de dire « 3 ans », mais « 3 ans pour la raison suivante »). Le rôle du DPO est alors de « challenger » la durée envisagée, pour vérifier qu'elle est proportionnée et qu'elle résisterait en cas de contrôle de la CNIL.

La durée de conservation peut être exprimée sous forme d'une durée absolue ou bien par rapport à une référence (au départ d'un collaborateur, dès la fin de relation commerciale avec un client, jusqu'à l'expiration des délais de recours, etc.). Elle doit être déterminée pour chaque traitement (et un traitement peut comporter plusieurs durées de conservation, applicables à certaines données traitées).

1 - https://www.cnil.fr/fr/sergic-sanction-de-400-000eu-pour-atteinte-la-securite-des-donnees-et-non-respect-des-durees-de
2 - Source CNIL « 1 an de RGPD en chiffres « : https://www.cnil.fr/fr/1-de-rgpd-une-prise-de-conscience-inedite

Le réflexe de toute MOA qui découvre le sujet est de se raccrocher à un référentiel. Certaines durées de conservation sont indiquées dans les textes de loi. De plus la CNIL, au fil de ses normes simplifiées, de ses autorisations uniques et de ses packs sectoriels, a indiqué de nombreuses références. Ainsi, dans le cas d'un dispositif de vidéosurveillance poursuivant un objectif de sécurité des biens, des lieux et des personnes, la conservation des images ne peut excéder un mois ; Les données relatives à gestion de la paie ou au contrôle des horaires des salariés peuvent être conservées pendant cinq ans ; un cookie ne peut avoir une durée de vie supérieure à treize mois ; La CNIL recommande que les coordonnées d'un prospect qui ne répond à aucune sollicitation pendant trois ans soient supprimées[3]. La Commission Nationale de l'Informatique et des Libertés est en train de convertir toute cette doctrine dans un référentiel unique (elle a, pour ce faire, consulté l'AFCDP pour recueillir l'avis des professionnels concernés), à paraitre prochainement. Ce référentiel aura-t-il valeur de rescrit (un responsable de traitement ne pouvant pas être sanctionné si la durée de conservation qu'il a déterminée est égale ou inférieure à celle de la CNIL) ? Mais l'on sait déjà que ce référentiel ne sera pas exhaustif (ce n'est pas son ambition), et la méthode décrite ci-dessus s'impose en tout cas (il est d'ailleurs sain de déterminer la durée de conservation par la réflexion et de vérifier seulement ensuite si celle-ci correspond bien à la référence).

Quelques idées fausses à tuer à ce stade : non, la loi Informatique et Libertés n'est pas « castratrice » et n'oblige jamais une entreprise à se priver de données dont elle a impérieusement besoin (y compris, par exemple, pour se protéger) ; non, il n'existe pas d'injonction contradictoire (entre plusieurs textes) ; non, une durée de conservation n'est pas forcément courte, pour preuve les 50 ans durant lesquels sont conservées par les services de santé au travail les fiches d'exposition des salariés exposés aux agents chimiques (et notamment l'amiante et les poussières de bois) et aux rayonnements ionisants pour éventuellement instruire des reconnaissances de maladies professionnelles et étayer d'éventuelles recherches en responsabilité (mais on aurait pu citer d'autres exemples dans le domaine de la retraite ou des successions).

La durée de conservation doit être portée à la connaissance des personnes concernées, comme en dispose l'article 13.2.a du RGPD : « *le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent : la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée...* ».

En fait, ce n'est pas une durée de conservation qu'il convient de déterminer, mais éventuellement trois, qui correspondent aux trois types d'archive. Pour aider les responsables de traitement, la CNIL a publié en 2005 une délibération[4] qui reste d'actualité et qui les décrit. Ainsi, le cycle de conservation des données à caractère personnel peut être divisé en trois phases successives distinctes : la base active (ou « archivage courant »), l'archivage intermédiaire et l'archivage définitif.

La durée qui est évoquée dans le RGPD (et qui doit être portée au registre des traitements tenu par le DPO et portée à la connaissance des personnes concernées) est celle d'utilisation courante des données ou autrement dit, la durée nécessaire à la réalisation de la finalité du traitement. Il peut être justifié ensuite que les données personnelles soient conservées en archivage intermédiaire, dans la mesure où il existe une obligation légale de conservation de données pendant une durée fixée ou que ces données présentent néanmoins un intérêt administratif, notamment en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables, notamment en matière commerciale, civile et fiscale. À titre d'exemple, une fois une transaction financière effectuée, les numéros de carte bancaire peuvent être conservés en « archivage intermédiaire » en cas d'éventuelle contestation de la transaction pour une durée de 13 mois conformément à l'article L133-24 du Code monétaire et financier. Enfin, sous réserve de garanties appropriées pour les droits et libertés des personnes concernées, certaines données peuvent être traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. C'est l'archivage définitif, domaine de l'archiviste, de l'article 5.1.e du RGPD et du Code du patrimoine.

À l'atteinte des durées de conservation de chacune de ces trois archives, les données peuvent être supprimées, anonymisées (afin notamment de produire des statistiques) ou versées dans la zone d'archive suivante – éventuellement avec un « floutage ». On parle du « sort des données ». Ainsi, on peut imaginer qu'un acteur du e-commerce conserve tous les détails d'un achat en ligne (par exemple un roman policier) pendant six mois, pour ne retenir les six mois suivants que l'achat d'un livre (et pas d'un CD), pour ne se souvenir ensuite que de l'achat d'un bien culturel (et pas d'une machine à café). Dans certains cas, l'archivage peut même être obligatoire. Un bailleur social peut ainsi archiver des données concernant d'anciens résidents pour être en mesure de satisfaire à un contrôle de la Mission Interministérielle d'Inspection du Logement Social[5] (MIILOS). Mais même cette archivage légal a une limite dans le temps : Les données archivées en prévision d'un éventuel contrôle de la MIILOS doivent, par exemple, être définitivement supprimées lorsque le contrôle ne peut plus être légalement opéré. De la même façon, des données archivées pour faire valoir un droit en justice doivent être supprimées lorsque cette action est prescrite.

Outre la détermination des durées de conservation, la véritable difficulté pour le DPO est d'obtenir que la réalité corresponde à la théorie... Ainsi, en application du principe de *Privacy by Design*, il doit vérifier que toute nouvelle application a été outillée pour « industrialiser » et faciliter les purges et dispose bien (si besoin) d'une zone d'archive intermédiaire. Il doit aussi exiger de la MOA Métier la production d'une procédure de purge qui définit clairement qui est responsable de la

3 - Source site web de la CNIL « Limiter la conservation des données » : https://www.cnil.fr/fr/limiter-la-conservation-des-donnees
4 - Délibération n°2005-213 du 11 octobre 2005 : Délibération portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel. https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017651957
5 - Source CNIL, Fiche « Durée de conservation et archivages des données » du Guide des bailleurs sociaux www.cnil.fr/sites/default/files/typo/document/FICHE3_Pack-Conf_LOGEMENT_SOCIAL_web.pdf

purge (chaque utilisateur ? un service local ? un département des services centraux ?). De plus, le DPO étant garant de la conformité, il doit réaliser ou faire réaliser des audits afin de vérifier que l'effacement des données est effective (et totale – toutes les copies devant également être effacées).

En résumé, la MOA Métier doit concrètement se poser les questions suivantes : jusqu'à quand ai-je vraiment besoin des données pour atteindre l'objectif fixé ? Avons-nous des obligations légales de conserver les données pendant un certain temps ? Devons-nous conserver certaines données en vue de nous protéger contre un éventuel contentieux ? Quelles informations doivent être archivées et selon quelles règles ? Pendant combien de temps ? De plus, il doit penser à formaliser une procédure de suppression des données et à outiller la nouvelle application en conséquence. Enfin, la MOA doit surtout se rapprocher du DPO, qui est toujours de bon conseil en la matière.

Le DPO, quant à lui, doit former les MOA Métier et les AMOA, et veiller à ce que les expressions de besoins et les cahiers des charges contiennent bien les exigences nécessaires sur ce sujet. Reste ensuite à obtenir que soient purgées les données au sein des traitements historiques : ce volet « *Privacy by reDesign* » est souvent le plus délicat, mais c'est un effort qui en vaut la peine.

Bruno Rasle
Délégué général de l'AFCDP

Mail : delegue.general@afcdp.net
Tel. +33 (0)6 1234 0884
Site Web : www.afcdp.net

Charte de déontologie du DPO Signataire

PRIX DE L'INNOVATION
EN MANAGEMENT JURIDIQUE

Comme chaque année, la Journée du Management Juridique a été l'occasion de remettre les Prix aux lauréats de cette 7ème édition du Prix de l'innovation en Management Juridique, organisée par le Village de la Justice. Durant 3 mois, les 6 équipes juridiques finalistes ont ainsi présenté leurs projets d'innovation à un jury de six professionnels, et au public grâce à de courtes vidéos.

Le 27 juin, Prix du Jury et Prix du public, ainsi qu'une mention spéciale, ont ainsi été décernés !

Prix du Jury
Ubisoft

Prix du Public
la Conserverie la belle-iloise

Mention spéciale
Direction juridique Social d'Air France