PAR CHRISTINE MAILLARD

# La Commission nationale de l'informatique et des libertés (Cnil) et les données de santé

**Depuis sa création en 1978, la Cnil, la plus ancienne des autorités administratives indépendantes, est un régulateur majeur de l'accès aux données de santé. Le nouveau règlement général de protection des données (RGPD), applicable en mai 2018, renforce son rôle et ses compétences.**

La loi « informatique et libertés » (encadré) garantit la protection des données par des obligations reposant sur le responsable du fichier (déclaration à la Cnil ou demande d'autorisation ; collecte des données de manière loyale et transparente ; assurer la sécurité des données) et par le respect des droits des personnes (à l'information, à l'accès, à la rectification et à l'opposition).
Elle interdit de traiter les données dites « sensibles », notamment celles relatives à la religion, à l'orientation sexuelle et à la santé, sauf à obtenir le consentement libre, spécifique et informé de la personne ou à être traitées dans le cadre d'activités de soins ou de prévention. Les données de santé peuvent également être traitées pour un motif d'intérêt public, par exemple, dans le cadre des vigilances ou d'entrepôts de données à des fins de recherche.
La Cnil régule toute personne qui met en œuvre un traitement de données informatiques, excepté les données complètement anonymisées, en vérifiant le respect de la loi. Depuis la loi santé 2016, les autorisations aux projets de recherche en santé doivent répondre à un intérêt public et sont soumises à un comité de protection des personnes ou à un comité d'experts, puis à la Cnil, qui les assortit d'une interdiction de réidentifier les personnes. La Cnil, qui entend simplifier les procédures, s'est engagée à répondre aux demandes dans les délais légaux, grâce à l'aide de l'Institut national des données de santé, secrétariat unique du Système national des données de santé (de l'Assurance maladie, des hôpitaux, du CépiDc et du handicap) créé par la loi Touraine.
Ses pouvoirs et missions sont variés : elle conseille le gouvernement, labellise, adopte des recommandations, garantit le droit d'accès au fichier de la police, exerce un pouvoir de contrôle sur place, instruit des plaintes, et peut sanctionner.

### Protection des données de santé

Premier enjeu, la sécurité informatique. Sachant que le manque de culture de sécurisation des systèmes d'information rend les établissements de santé très sensibles aux attaques informatiques, Thomas Dautieu avertit que *« tous les appareils nomades très peu sécurisés feront l'objet d'attaques informatiques, et si celles-ci portent sur les dispositifs médicaux connectés (défibrillateurs implantables, pompes à insuline), des conséquences mortelles sont à craindre »*. D'où la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) portée par le ministère de la Santé, qui travaille à un référentiel opposable aux établissements, avec une obligation de notification des failles aux agences concernées (Asip, ARS).

**LE RESPONSABLE DU FICHIER N'AURA PLUS À LE DÉCLARER À LA CNIL**

Deuxième enjeu, l'impact majeur du RGPD sur les professionnels de santé. Alors que la loi de 1978 avait été suivie en 1995 d'une directive européenne à transposer dans chaque pays de l'Union, le RGPD, publié en 2016, est directement applicable, sans transposition selon les pays, le 25 mai prochain. Ses trois idées-forces sont de : crédibiliser les autorités européennes (elles devront vraiment coopérer ou, en cas de désaccord, voter) ; renforcer le pouvoir de sanction de la Cnil (amendes jusqu'à 20 millions d'euros) et les droits des personnes (droit à la portabilité : *« il sera possible de récupérer ses données et les porter chez un autre opérateur »*) ; responsabiliser les acteurs. Le responsable du fichier n'aura plus à le déclarer à la Cnil, mais devra prouver à tout moment sa conformité, le recueil du consentement – la Cnil n'aura plus à démontrer qu'il n'a pas été obtenu –, et la protection des données. À la Cnil de se réinventer, en formant les futurs délégués à la protection des données sur lesquels elle s'appuiera et en renforçant ses contrôles.
Troisième enjeu, face au défi de l'intelligence artificielle, le RGPD reprend un principe prévu dans la loi de 1978 (« une machine ne peut donner une décision sans intervention humaine ») : les personnes doivent être informées de l'utilisation d'un algorithme, et pouvoir s'opposer à ce qu'une décision médicale soit établie par la seule machine. Ces éléments font partie de la réflexion de la Cnil sur l'éthique dans le numérique qui, cette année, porte sur les algorithmes (loi pour la République numérique 2016).

## LOI INFORMATIQUE ET LIBERTÉS

**Conçue en 1978 en réaction au projet gouvernemental d'identifier tous les citoyens par un identifiant unique (le Nir), cette loi prévoit les obligations des créateurs de fichiers et les droits des personnes dont les données sont traitées. Le principe clé de la protection des données est le principe de finalité d'où découlent les autres obligations : détermination de la durée de conservation, de la pertinence des données, de la légitimité des destinataires, etc. La philosophie de la loi est de traiter le moins de données possible, pendant le moins de temps possible, avec le moins de destinataires possible. « Il faudrait que sa prochaine révision coïncide avec l'application du RGPD. »**

D'après la conférence de THOMAS DAUTIEU (tdautieu@cnil .fr), direction de la conformité à la Cnil, www.cnil.fr