À quatre mois de leur ouverture, le délicat chantier de la sécurisation des données de santé

10 janv. 2017, PAR Le Nevé Soazig

Fotolia

À quatre mois du lancement du Système national des données de santé (SNDS), s'ouvre le chantier de la sécurisation de l'accès à cette immense base d'informations personnelles. Pour préparer le terrain, des députés ont auditionné, le 10 janvier, Kamel Gadouche, directeur du Centre d'accès sécurisé aux données.

Avec le développement des objets connectés, le nombre de données de santé sera multiplié par 50 dans les prochaines années. C'est ce qu'a prédit, le 10 janvier, le député Pierre Morange, qui copréside la mission d'évaluation et de contrôle des lois de financement de la Sécurité sociale (Mecss) de l'Assemblée nationale.

En vertu de la loi "Santé" de janvier 2016, visant notamment à ouvrir plus largement l'accès aux données de santé, l'Agence technique de l'information sur l'hospitalisation (Atih) a choisi le Centre d'accès sécurisé aux données (CASD) pour mettre à la disposition des chercheurs, *data scientists* et consultants les données du Programme de médicalisation des systèmes d'information (PMSI).

Attaques informatiques en perspective

D'ici le mois d'avril, cette base de données PMSI sera en effet versée au futur Système national des données de santé (SNDS) au même titre que les données de santé de l'assurance maladie obligatoire (base Sniiram) *[lire notre article]*. Soit 1,2 milliard de feuilles de soins, 500 millions d'actes médicaux et 11 millions d'hospitalisations par an.

"Pas moins de 26 000 attaques informatiques ont été repoussées par le ministère de la Défense en 2016, a rappelé Pierre Morange. *J'ai de la peine à imaginer que ce ne sera pas le cas aussi pour les données sociales. Ces données s'échangent contre rançon. C'est une nouvelle économie criminelle qui s'est développée."*

Un tiers de confiance

"Gouvernance", "qualité des coffres forts informatiques" de la CNAMTS et du PMSI, *"crainte de la vampirisation de données"* : à six mois de l'échéance et pour tenter de dégager la marche à suivre pour constituer un SNDS réellement sécurisé, la Mecss a interrogé Philippe Cunéo, directeur général du Groupe des écoles nationales d'économie et statistiques (Genes), et Kamel Gadouche, directeur du CASD.

Plusieurs producteurs de données, tels que l'Insee, la direction générale des finances publiques, les ministères du Travail, de la Justice ou encore de l'Éducation nationale, recourent d'ores et déjà au CASD pour compiler et assurer la protection des données sensibles diffusées.

"On se comporte comme un tiers de confiance, avec un lien contractuel avec les producteurs de données", a expliqué Kamel Gadouche. Un contrat lie également le Centre à ses utilisateurs, au nombre 1 000 actuellement (pour 400 projets de recherche en cours). Les personnes habilitées disposent ainsi d'un boîtier à carte à puce biométrique qui leur permet d'accéder aux bases de données, boîtier qu'ils s'engagent à installer dans un bureau fermé, *"et pas dans le hall de leur établissement"*. D'autres clauses prévoient que l'utilisateur est seul devant son écran d'ordinateur et qu'il quitte la session lorsqu'il s'absente…

Contrôles ex ante ou ex post ?

Le CASD parviendra-t-il à gérer aussi bien la masse des données du futur Système national des données de santé ? Pas si sûr : alors que le Centre procède à des contrôles *a priori* des utilisateurs, la loi "Santé" s'oriente, elle, vers la pratique d'un contrôle *a posteriori,* dont les modalités restent encore à définir, dans un

arrêté à venir. *"C'est une différence majeure,* selon Philippe Cunéo, le directeur général du Groupe des écoles nationales d'économie et statistiques. *On ne va pas faire ceinture et bretelles* (ex ante *et* ex post) ! *Il va falloir se mettre d'accord et attendre la préconisation de la Cnil."*

À ses yeux, le contrôle *a priori* fonctionne bien. *"Une fois entrés dans la « bulle », les chercheurs y écrivent leur article. Ils ont appris une nouvelle façon de travailler. Il n'est plus besoin de sortir les données de cette bulle du CASD. Seuls en sortent les articles une fois rédigés par les chercheurs."*

1 200 euros par an et par chercheur

L'unique limite, c'est le délai d'accès aux données (six mois en moyenne), qui peut pousser des utilisateurs à demander un contrôle *a posteriori.* Une démarche que Philippe Cunéo juge risquée : *"Au Danemark par exemple, on procède par contrôles aléatoires et il peut arriver que l'on découvre alors qu'un dossier confidentiel est sorti."*

Dernière interrogation soulevée par la Mecss, le modèle économique qui résultera d'une intégration du SNDS. L'exemple actuel du CASD montre que chaque utilisateur paie 800 euros par an en moyenne pour un coût de revient équivalent à 1 200 euros, quel que soit le nombre de données utilisées par le chercheur. Total : un budget de 2 millions d'euros annuels est nécessaire.

"Notre dispositif technique peut monter en échelle, a assuré Kamel Gadouche. The sky is the limit ! *Sauf dans le cas de travaux très particuliers qui seraient demandés à partir de la base Sniiram par exemple. Il faudrait alors penser à de nouvelles infrastructures."*

Avant toute consultation de données, un contrôle *ex ante*
Au Centre d'accès sécurisé aux données (CASD), les chercheurs doivent d'abord présenter leur dossier à un "comité du secret" (composé d'un conseiller d'État, Jean Gaeremynck, de producteurs de données, de la Cnil, des représentants des syndicats, de chercheurs, des Archives de France et de représentants de l'Assemblée nationale et du Sénat) qui se réunit tous les trois mois. Les utilisateurs suivent ensuite une "séance d'enrôlement" qui vise à les informer et à leur délivrer une carte d'authentification, après signature d'un contrat d'utilisation.
Selon Philippe Cunéo, directeur général du Groupe des écoles nationales d'économie et statistiques (Genes), *"pour les questions vitales, comme c'est le cas d'une épidémie, il faut qu'un petit nombre de personnes identifiées ait accès à un maximum d'informations. Mais peu de gens, car il faut pouvoir tracer les accès et sorties que ces personnes ont engagés, avec un haut degré de responsabilité"*. Le directeur plaide pour ne distinguer que deux catégories : ce tout petit nombre de personnes habilitées et le reste. *"Il est dangereux d'imaginer trop de niveaux de confidentialité différents, car c'est très difficile à mettre en œuvre"*, a-t-il prévenu.