PROTECTION DES DONNÉES PERSONNELLES

RGPD : le médico-social loin du compte

Deux ans après la mise en place de la réglementation européenne sur la protection des données, quelle est l'avancée de ce chantier au sein des établissements et services du secteur social et médico-social ? Le chemin à parcourir vers une culture de la protection des données et de la sécurité informatique semble encore très long.

DR

LE 2 JUILLET DERNIER, L'AGENCE NATIONALE D'APPUI À LA PERFORMANCE DES ÉTABLISSEMENTS DE SANTÉ ET MÉDICO-SOCIAUX (ANAP) a mis en ligne un kit composé d'un autodiagnostic (composé de 49 questions) permettant aux directeurs de structures d'établir un état d'avancement de la mise en conformité avec le règlement général sur la protection des données (RGPD) ainsi que d'un corpus détaillant les exigences réglementaires. Entré en vigueur en mai 2018, le RGPD a renforcé l'encadrement réglementaire de la protection des données personnelles (dont celles de santé), couvert jusqu'alors par la loi dite « informatique et libertés » de 1978. Deux ans après, où en sont les établissements et services sociaux et médico-sociaux (ESSMS) dans sa mise en œuvre ?

> « Une institution ne peut pas mettre en place le RGPD si elle n'a pas convaincu tous ses acteurs du bien-fondé de la démarche, des règles à respecter, des risques »

Avocat spécialiste du secteur et associé du cabinet Accens Avocats chargé du RGPD, Pierre Naitali observe *« une approche très hétérogène de la mise en conformité »*. Selon lui, quatre groupes peuvent être distingués. Tout d'abord, *« ceux qui n'ont rien fait, et il en existe un nombre assez significatif »*. Y compris de grosses associations. Ensuite, *« ceux qui ont désigné un délégué à la protection des données* [DPD, ou Data Protection Officer (DPO)] *pour répondre à une obligation facialement facile à contrôler, mais qui, en termes de mise en conformité, n'ont rien fait »*. Une troisième catégorie compte *« tous ceux qui ont désigné comme DPD leur directeur informatique – ce qui est illégal – ou leur responsable qualité »*. Ces ESSMS ont mené à bien *« un embryon d'actions »*. Mais l'avocat ajoute : *« S'ils subissent demain un contrôle de la Cnil* [Commission nationale de l'informatique et des libertés], *il est probable que ce qu'ils ont mis en place amènera à un grand nombre d'injonctions. »* Vient enfin le *« club »* des bons élèves, qui ont pris le dossier RGPD à bras le corps et l'ont intégré dans leur fonctionnement.

UNE DÉMARCHE « COLLECTIVE ET ORCHESTRÉE »

Pierre Naitali égrène les causes de tels retards ou manques : l'absence de moyens ; le refus des autorités de tarification et de contrôle (ATC) de financer ce chantier ; le manque d'appétence de certains dirigeants sur les questions informatique ; l'absence de personnes ressources ; le manque de temps. *« Enfin, l'un des facteurs principaux des difficultés est que l'information sur le RGPD est extrêmement disséminée »*, égrène Pierre Naitali.

De l'avis de Myriam Vallin, consultante au cabinet de conseil Handiness consacré à la transition numérique du secteur médico-social, l'avancement de la démarche RGPD est lié à la maturité numérique de l'organisation. *« L'élément réellement facilitateur est la présence d'une démarche qualité,* juge-t-elle. *Une institution ne peut pas mettre en place le RGPD si elle n'a pas convaincu tous ses acteurs du bien-fondé de la démarche, des règles à respecter, des enjeux, des risques autour de l'utilisation du numérique. »* Et d'ajouter : *« Considérer le RGPD comme un projet à part est une erreur qui générera à coup sûr l'échec de la démarche. Le sujet RGPD doit être présent dans tous leurs projets puisque les établissements et services traitent des données dès qu'ils font quelque chose. Le RGPD est transversal, il ne concerne pas le seul DPO mais l'ensemble des acteurs au sein des ESSMS dans leurs pratiques professionnelles. Dès qu'on lance un projet, il faut se poser la question de la collecte des données. La sensibilisation à la protection des données doit être collective et orchestrée, afin que les questions "qui ?", "quoi ?", "où ?", "quand ?", "comment ?", "combien ?" et "pourquoi ?" soient à l'esprit de tous les opérateurs. »*

De son côté, Pierre Naitali rappelle que la désignation du DPO est la partie visible de l'iceberg. *« Le gros du*

travail de mise en conformité est de prendre le temps d'acculturer les collaborateurs de l'organisme gestionnaire et des établissements à ce qu'est le RGPD. On ne traite pas n'importe comment les données des usagers, des salariés. Il faut également du temps pour recenser les données dans les établissements en interne ou en externe, établir les registres de traitements, faire les analyses d'impact. »

Principe majeur du RGPD issu de l'article 5 du règlement européen, l'*accountability* (littéralement, « responsabilité ») désigne, selon la Cnil, *« l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données »*. Mais cette obligation implique également pour les organismes traitant des données personnelles d'être en mesure de démontrer, à tout moment, leur conformité au RGPD. Une responsabilisation des acteurs qui laisse peu de place à l'amateurisme dans la mise en application du règlement européen.

Myriam Vallin insiste sur le fait que la mise en conformité est un processus continu. *« Certes, le RGPD ne traite pas que des données numériques. Mais c'est au niveau numérique qu'elles deviennent exponentielles,* explique-t-elle. *L'utilisation accrue du numérique et l'évolution des techniques engendrant une augmentation croissante du volume de données et de modalités de traitement. Compte tenu de la multiplicité des acteurs, des parcours, des prises en charge, le RGPD est de la haute couture et non du prêt-à-porter. »* La consultante déplore toutefois le fait que peu de formations initiales aient pris à cœur d'équiper les futurs professionnels du secteur de cette nouvelle compétence : *« On attend que les référentiels de formation intègrent la matière. Tant que l'on n'aura pas réglé ce problème de formation, la mise en œuvre du RGPD sera compliquée. »*

> « Compte tenu de la multiplicité des acteurs, des parcours, des prises en charge, le RGPD est de la haute couture, et non du prêt-à-porter »

DR

SIX PRIORITÉS À RESPECTER

Selon la Commission nationale de l'informatique et des libertés (Cnil), pour répondre aux exigences du RGPD, six points sont à respecter :

- la désignation d'un délégué à la protection des données (DPD), qui exercera une mission d'information, de conseil et de contrôle interne ;
- le recensement des données personnelles manipulées et l'évaluation des risques que leurs traitements font peser sur les droits et les libertés des personnes concernées ;
- l'identification des actions à mener pour leur respect ;
- la définition de procédures internes garantissant la protection des données, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de leurs traitements ;
- la mise en place de procédures internes pour gérer les risques (analyse d'impact) ;
- la constitution et le regroupement de la documentation établissant la conformité des actions menées pour assurer une protection des données en continu.

Les organismes gestionnaires devront être capables de démontrer *(accountability)* auprès de la Cnil la conformité des mesures.

DES SANCTIONS À VENIR

En cas de manquement dans la protection des données, les textes prévoient des sanctions financières. Pour rappel, les amendes peuvent aller jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires mondial annuel si cette seconde valeur est supérieure. Les sanctions administratives peuvent être complétées par des condamnations pénales. De plus, toute violation du RGPD peut engager la responsabilité du responsable du traitement (préjudice moral et matériel subi par la personne concernée), entraîner une perte de confiance des usagers envers l'établissement et porter atteinte à son image. En mars dernier, le centre national d'addictologie irlandais a été condamné à une amende administrative d'environ 20 000 € en raison d'une violation constatée de données et d'un manque général de sécurisation du système d'information, malgré les nombreuses améliorations mises en place par l'établissement.

« Ceux qui considèrent que la CNIL ne fera preuve d'aucune sévérité à l'égard du secteur social et médico-social si celui-ci ne respecte pas le RGPD se trompent profondément. Car nous évoluons dans un secteur qui est particulièrement concerné par la notion de données sensibles. La Cnil aura à cœur de protéger les données des personnes », prévient Pierre Naitali. Et d'insister : *« A brève échéance, quand il y aura des problèmes de mise en œuvre, elle appliquera la même échelle de sanctions que pour les entreprises d'autres secteurs d'activité. Le RGPD est une réglementation d'essence européenne. Et l'Europe raisonne toujours par l'effectivité de la mise en œuvre des droits des personnes, et non sur le fait d'avoir mis ou pas des procédures. »*

Myriam Vallin considère également que l'immunité dont pensent bénéficier certains retardataires est *« une illusion d'arrière-garde ». « La bombe à redou-*

ter n'est pas la sanction financière mais l'interdiction de traiter des données. Si le partage et le transfert d'informations sont nécessaires à une bonne prise en charge des personnes et font partie intégrante du travail d'une association et que celle-ci ne se dote pas des outils nécessaires pour le faire, alors elle ne fait pas correctement son travail. Dans ce cas, une autorité de tarification et de contrôle pourra lui dire : "Vous n'avez plus le droit de traiter des données, et donc on va vous faire reprendre par une autre association."» L'urgence de la mise en conformité avec le RGPD va aller en s'accélérant pour les ESSMS. En 2020, l'Anap a étoffé son tableau de bord de la performance dans le secteur médico-social en y intégrant des indicateurs sur le RGPD. Par ailleurs, le prochain référentiel d'évaluation des structures en préparation à la Haute Autorité de santé (HAS) va également tenir compte du respect de la réglementation sur la protection des données personnelles.

Selon une enquête menée par Data Legal Drive, la crise du Covid-19 a servi, dans une certaine mesure, de catalyseur aux entreprises dans leurs travaux de mise en conformité. L'étude précise ainsi que près de 40 % des DPO et juristes interrogés disent avoir mis à profit le confinement pour *«traiter les sujets de fond de la mise en conformité RGPD de leur entreprise, et en particulier, pour près de la moitié des répondants, la mise à jour du fameux registre des traitements»*. CEO de Data Legal Drive & associé du Cabinet DS Avocats, Sylvain Staub analyse : *«Aux premiers jours de la crise sanitaire, certains ont pu croire que la mise en conformité RGPD serait reléguée aux calendes grecques. En réalité, c'est le contraire qui s'est produit. La mise en place du confinement a massivement permis aux entreprises de prendre pleinement conscience du chemin à parcourir : le télétravail massif suppose une (ré)organisation RH poussée, avec des questions de droit social et de vie privée, et une (re)mise à niveau des procédures de sécurisation des données.»*

Pierre Naitali souligne : *«La crise sanitaire a fait ressortir des problématiques qui existaient déjà dans le secteur social et médico-social : télétravail, échanges d'informations entre organismes, utilisation du matériel personnel par des professionnels, gestion des mots de passe…»* Tandis que Myriam Vallin se satisfait : *«La crise sanitaire aura peut-être amené les organisations technico-septiques à se remettre en cause et à comprendre que le numérique est un passage obligé mais bénéfique. On a gagné deux ans.»* Et Pierre Naitali de conclure : *«Le RGPD est d'abord une question de respect des individus, des usagers, des salariés, de leurs droits, de leur vie privée. Cette question de respect, déjà présente dans la loi du 2 janvier 2002, est traitée ici sous un nouvel angle. Pour les établissements qui comprennent qu'il faut mettre en place des outils, et surtout cette culture de la protection des données, le RGPD n'est pas une usine à gaz.»* ●

NADIA GRARADJI

DR

INVESTISSEMENT

600 M€ POUR LE NUMÉRIQUE DANS LE MÉDICO-SOCIAL

«INVESTIR MASSIVEMENT POUR RATTRAPER LE RETARD DANS LA MODERNISATION, L'INTEROPÉRABILITÉ, LA RÉVERSIBILITÉ, LA CONVERGENCE ET LA SÉCURITÉ DES SYSTÈMES D'INFORMATION EN SANTÉ.» Le 22 juillet, lors de la clôture du Ségur de la santé, Olivier Véran, ministre des Solidarités et de la Santé, a annoncé une enveloppe de 2 milliards d'euros consacrée au développement du numérique en santé. Ce même plan d'investissement prévoit 600 millions d'euros sur cinq ans pour permettre aux établissements médico-sociaux d'investir *«dans les équipements de base, les logiciels socles et les services d'échange»*. Jusqu'à présent, le programme « ESMS numérique » disposait d'un *«fonds d'amorçage de 30 millions d'euros»* initialement prévu par la Caisse nationale de solidarité pour l'autonomie (CNSA).

Comme le souligne l'Agence du numérique en santé, le développement des outils numériques reste inégal dans le secteur médico-social, du fait, entre autres, *«de l'hétérogénéité des publics concernés, des structures impliquées et du sous-investissement de la puissance publique en comparaison avec le secteur sanitaire»*. (1) Cette enveloppe de 600 millions d'euros a donc pour objectif de donner *«une impulsion déterminante à la modernisation des outils numériques dans ce secteur»*, en particulier à la généralisation du dossier de l'usager informatisé (DUI), qui est au cœur des systèmes d'information.

Dans un courrier commun en date du 9 juillet adressé à la délégation du numérique en santé (DNS), Nexem, la Fehap et l'Unapei ont porté leurs interrogations autour du plan « ESMS numérique » et de son déploiement. *«Quel accompagnement est prévu pour les gestionnaires – et notamment ceux de petites tailles – pour accéder au marché du DUI ? Pour formaliser leurs besoins, notamment ? Quelle garantie pouvez-vous apporter pour une réelle prise en compte des spécificités sociales et médico-sociales du marché national du DUI ?»*, interrogent-elles. Les fédérations rappellent également la nécessité d'inclure dans les travaux le secteur social, *«grand oublié du chantier national numérique»*. Un rendez-vous avec la DNS est prévu fin juillet. ● N. G.

(1) L'Agence du numérique en santé a publié sur son site Internet (esante.gouv.fr) un document intitulé « Trajectoire numérique adaptée au secteur médico-social », soumis à la concertation et aux contributions des acteurs jusqu'au 25 septembre.