OPTION/BIO
L'ACTUALITÉ DU PRATICIEN BIOLOGISTE
Périodicité : Mensuel

Date : NOV/DEC 17
Journaliste : Serge Benaderette

à la une

Traitement des données numériques : les biologistes en quête de protection maximale

Après le 25 mai 2018, toute entreprise qui n'aura pas renforcé la sécurisation des données qu'elle traite s'expose, selon le règlement européen de protection des données, à de lourdes amendes. Prenant les devants, le syndicat des biologistes (SDB) entend doter les LBM d'outils pour s'y conformer. Au cours de sa 1re journée scientifique, le SDB vient de faire le point sur les préparatifs d'un code de conduite destiné à aider la profession à se mettre dans les clous des nouvelles obligations.

© S Bernadette

Les biologistes veulent renforcer leur cybersécurité. Le 10 octobre, Bruno Gauthier (au micro) a annoncé les outils que la société française d'informatique de laboratoires (SFIL) prépare à cet effet.

La sphère de l'e-santé va connaître de notables adaptations (et sans délais) à partir du 25 mai 2018 dans toute l'Union européenne (UE), avec la mise en application du règlement unique sur la protection des données personnelles (RGPD) résultant de quatre ans d'intenses débats au Parlement européen. Qu'édicte-t-il ? Pas moins de 400 obligations introduites par 99 articles et 78 considérants. Paru au journal officiel de l'UE le 4 mai 2016, le texte s'impose à tous, à la France comme aux 27 autres États membres, chacun ayant la charge d'intégrer sur son sol les nouvelles dispositions réglementaires et de mettre les systèmes d'information et leurs traitements en conformité avec les nouvelles obligations de sécurité des données dématérialisées (data), de santé en particulier.

Gros producteurs de flux de résultats et de comptes rendus d'examens cyber, les biologistes médicaux (BM) comptent parmi les créateurs et hébergeurs de données personnelles de santé et de traitements sensibles parmi les plus impactés. Cette prise de conscience les met sur le pont face à l'urgence. Très avancés au niveau de la maîtrise des systèmes d'information (SI) ils se sont, au lendemain du congrès de la société française d'informatique de laboratoires (SFIL) les 9 et 10 mars à Chambéry (voir *OB n° 559-560*),emparés des modifications qu'induisent les nouvelles contraintes réglementaires sur leur fonctionnement et procédures. Pour anticiper les échéances de cette injonction numérique, la SFIL, répondant à un appel d'offres de la commission

Traitement des données numériques : les biologistes en quête de protection maximale

nationale informatique et liberté (CNIL), s'était dès juin, portée candidate dans l'écriture d'un référentiel sectoriel destiné à aider les laboratoires de biologie médicale (LBM) à se mettre en conformité avec le nouveau règlement européen particulièrement sanctionnant en cas de défaillance. D'où la production d'un code de (bonne) conduite dont la première version sera validée mi novembre, livrée à la CNIL, puis mise à disposition des LBM a confirmé Bruno Gauthier de Bio 86, membre du bureau du syndicat des biologistes (SDB), trésorier de la SFIL. Il vient, parmi les quatre ateliers de la première journée scientifique que le SDB a organisée le 10 octobre à Paris, d'animer celui consacré à l'actualité de la mise en œuvre des réglementations informatiques nationales et européennes.

L'accompagnement CNIL : une opportunité exceptionnelle

S'agissant du règlement européen, un code de conduite est en chantier pour « *répertorier, processus par processus, l'ensemble des exigences juridiques et techniques qui vont s'appliquer aux différents métiers dans les LBM* » a précisé Marguerite Brac de la Perrière qui représentait le cabinet Lexing Alain Bensoussan avocats, spécialisé en droit numérique. La SFIL s'est attachée ses compétences de juriste, tout comme celles aussi du cabinet Provadys, spécialiste des techniques de protection des données et de cybersécurité, représenté à l'atelier par Olivier Pantaléo. Ces deux opérateurs vont aussi assister la SFIL pour le second chantier qui consistera, en novembre et décembre, à élaborer le projet de *privacy impact assesement framwork* (PIAF) en l'adaptant à la biologie médicale (BM). Constitutif du dispositif réglementaire du RGPD, ce document doit permettre au LBM qui le met en œuvre, de démontrer qu'il s'est mis en conformité. Opposable et personnalisé par domaine d'activité, il recense les principes fondamentaux fixés par la loi, les contrats types et permet l'analyse des risques sur la vie privée des personnes concernées par les traitements, en l'occurrence, ici, les patients du LBM.

L'amende : 4 % du chiffre d'affaires

Alors que les échéances approchent, il s'agit de doter l'entreprise biologique des moyens de prendre les mesures techniques et organisationnelles appropriées pour garantir un haut niveau de protection des données. En d'autres termes le PIAF a pour vocation d'anticiper les risques encourus diagnostiquant la vraisemblance des incidents potentiels et de leur gravité, de les identifier, d'en évaluer la proportionnalité. Il revient à chaque LBM d'analyser sa situation grâce à ce document opérationnel qui, mis à disposition par la SFIL - sera « *demandé par la CNIL ou par toute autre organisation dès lors que se produira un incident de sécurité* » prévient Olivier Pantaléo. Il va y avoir un avant et un après 2018. Pour tout nouveau traitement le LBM devra démontrer qu'il est en capacité de prendre les bonnes décisions et de gérer correctement les risques. L'analyse d'impact devra intervenir dès la conception d'un traitement, d'un système d'information, d'une application selon le principe du *privacy by design*, l'un des fameux volets du RGPD, et qui va drastiquement contraindre les entreprises à s'adapter. Car celles qui ne seront pas conformes s'exposent à une amende qui peut atteindre 20 millions d'euros ou 4 % du chiffre d'affaires monde.

Les parades aux cyberattaques

L'objectif de la SFIL est, après avoir testé sur le terrain l'efficience du dispositif, de mettre à disposition des LBM la mallette contenant les outils nécessaires qui à partir de janvier 2018 leur permettront de rentrer dans la démarche et d'intégrer la réglementation européenne sur la définition d'un traitement.

L'esprit du RGPD est d'accorder de nouveaux droits aux citoyens et de nouveaux devoirs aux acteurs de santé. Depuis mai, *conformément à celui-ci*, la CNIL a allégé les formalités préalables des demandes d'autorisation administratives d'agrément de traitement des données, au profit d'un régime de déclaration. Ce qui va la rendre des plus vigilante sur les conditions de mise en œuvre du traitement des données de santé tout particulièrement sur le recueil du consentement des personnes, en procédant à des contrôles en aval

Est-ce l'arme atomique pour se prémunir contre les cyberattaques ? Le RGPD renforce en tout cas les obligations de protection des entreprises en matière de cybersécurité. « *Ce ne sera pas du luxe face à des bandes malfaisantes organisées pour hacker tous les systèmes de grandes ou petites entreprises dès lors qu'ils peuvent s'engouffrer dans une faille* » explique Olivier Pantaleo. Sur les 68 % d'entreprises qui ont fait l'objet d'une attaque au cours des 24 derniers mois la moitié était des TPE-PME. Globalement en 2015 la facture des cyberattaques s'est élevée en France à 3,7 milliards d'euros et s'est accrue de 30 % en 2016. Pourquoi ? Parce qu'il est plus facile de pirater un traitement de données que d'attaquer une banque. En l'occurrence les LBM en ont déjà été victimes. Le règlement européen freinera-t-il la cybercriminalité ? Les BM se donnent, semble-t-il, les moyens d'en réduire les risques dans leur sphère. Stratégie nationale de santé oblige ! La SFIL élargit par ailleurs ses investigations aux échanges et au partage des données médicales au sein de l'équipe de soins coordonnée. D'où son colloque interprofessionnel, le 16 novembre à Paris, sur ce versant de la dématérialisation. I

SERGE BENADERETTE
Journaliste, Paris
serge.benaderette@orange.fr