Cloud Act : les nuages s'amoncellent-ils sur la protection des données de santé françaises ?

C'est le 23 mars 2018 qu'a été promulguée la loi fédérale américaine *Clarifying Lawful Overseas Use of Data Act*, dite « Cloud Act ». Ce texte autorise les pouvoirs de police des États-Unis (FBI, forces de l'ordre, etc.) à accéder aux données hébergées sur les serveurs des fournisseurs américains de services Cloud et de leurs filiales à l'étranger. Ce qui leur confère un droit de regard sur les données produites par les établissements de santé français qui ont opté pour un fournisseur américain de service Cloud. Faut-il s'en inquiéter ?

Décrypter les « secrets » des données à caractère personnel est une préoccupation ancienne des autorités américaines. Traduit en français, « *Clarifying lawful overseas use of data act* » signifie « loi clarifiant l'utilisation légale des données à l'étranger », prévue par le Stored communications Act, voté en 1986. Ce texte faisait suite au refus de Microsoft Irlande de communiquer des informations sur ses serveurs dans le cadre d'une affaire criminelle. Jusqu'où va le Cloud Act ? Octroie-t-il un blanc-seing aux pouvoirs des polices américaines ? « *Le champ d'application semble large,* observe Me Jeanne Bossi Malafosse, responsable du département Données personnelles et coresponsable du département Sciences du vivant au cabinet parisien Delsol Avocats. *Mais, le recours à ce texte est soumis à un certain nombre de conditions.* » Toute réquisition de données requiert l'intervention d'un juge, même si certains rappellent que l'indépendance des juges américains qui sont élus est sujette à caution. « *Ce biais peut introduire une suspicion d'intérêts personnels et financiers* », relève l'avocate. Néanmoins, cette obligatoire intervention d'un magistrat constitue une première limite au Cloud Act. D'autres filtres existent comme les *executive agreements*, ces accords particuliers conclus antérieurement entre les États-Unis et un pays étranger. « *Le prestataire pourra s'en prévaloir pour éventuellement contester, dans un délai de 14 jours, la demande de transmission de données* », complète Me Jeanne Bossi Malafosse. Et, bien sûr, il y a le RGPD qui constitue une autre garantie.

Le RGPD comme garde-fou

Le règlement général sur la protection des données (RGPD) s'applique à toute donnée à caractère personnel de résidents du territoire européen, y compris quand le responsable de collecte et de traitement de ces données se trouve hors de l'Union européenne. Autre élément protecteur, le Privacy Shield, accord négocié en 2016 entre les États-Unis et l'Union européenne et qui accorde aux données des citoyens européens une protection équivalente à celle des citoyens américains. « *Au besoin, la Commission européenne pourra faire valoir cet accord, non pour bloquer le Cloud Act, mais pour en circonstancier les demandes* », précise Me Jeanne Bossi Malafosse. D'autre part, l'Asip Santé réfléchit à inclure dans la procédure de certification des hébergeurs de données de santé une condition obligeant un hébergeur américain à respecter le RGPD. Assurément, RGPD et Cloud Act vont s'entrechoquer, prédit l'avocate spécialiste des données à caractère personnel, rappelant que l'article 28 du texte européen a considérablement renforcé les obligations des prestataires, américains compris, à l'égard de leurs clients. Et d'insister : le Cloud Act n'est pas un droit permanent et sans condition d'accès au système d'information d'un prestataire américain. Alors, non, des escadrons d'hélicoptères numériques transportant dans le secret d'une nuit elle-même numérique des troupes de *marines* tout aussi numériques ne viendront pas se servir à volonté dans les coffres (numériques pour de vrai cette fois) hébergeant les données d'hôpitaux français. Toute demande des autorités américaines, dans le cadre exclusif d'une affaire criminelle, devra, quoi qu'il en soit, se référer aux accords bilatéraux existants sur les conditions d'échange de données entre États signataires.

Me Jeanne Bossi Malafosse, responsable du département Données personnelles et coresponsable du département Sciences du vivant au cabinet 0parisien Delsol Avocats.

Wait and see

Faut-il malgré tout y regarder à deux fois pour confier à un prestataire américain ses données à caractère personnel ? Le Cloud Act créant des cas particuliers de demandes d'accès aux données par les autorités judiciaires américaines, Me Jeanne Bossi Malafosse évoque la possibilité de recourir à des prestataires répondant au référentiel SecNumCloud de l'Anssi, l'Agence nationale de la sécurité des systèmes d'information. Ce référentiel favorise les Clouds publics souverains, avec sécurisation des bases de données en France. Reste que ce texte est récent. « *Nous manquons de recul. Il faut attendre les cas concrets pour avoir une vision de l'étendue de ses effets* », souligne l'avocate. Et si le Cloud Act fait peur, l'arsenal juridique français et européen est suffisamment étoffé pour faire respecter la confidentialité des données.

Pierre Derrouch