Cloud : les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles

19 juillet 2024

Dans son état actuel, le projet de certification européenne pour les services de cloud (EUCS) ne permet plus aux fournisseurs de démontrer qu'ils protègent les données stockées contre tout accès par une puissance étrangère, contrairement à la qualification SecNumCloud en France. La CNIL appelle à rehausser le niveau de protection des données personnelles de cette certification en réintroduisant de telles garanties.

Des données sensibles qui doivent être particulièrement protégées

Les données stockées par une entreprises soumise à un droit extra-européen, comme c'est le cas des hébergeurs dont les sociétés mères sont situées aux États-Unis, peuvent être exposées à un risque de devoir communiquer des données aux autorités publiques de ce pays. Ce risque est le plus souvent considéré comme limité, en particulier pour des données non sensibles confiées à des prestataires relevant de « pays adéquats » en termes de protection des données personnelles. C'est notamment le cas pour les États-Unis, qui constituent un « pays adéquat » depuis la décision de la Commission européenne du 10 juillet 2023 (dans les conditions précisées par le *Data Privacy Framework*). Cependant, une protection renforcée s'impose pour les traitements de données les plus sensibles (par exemple de grandes bases de données de santé, de données d'infractions ou encore de données relatives à des mineurs), pour lesquels les données hébergées dans l'Union européenne **ne devraient pas être sujettes à un risque d'accès non autorisé par des autorités d'États tiers.**

Dans ce cas, la CNIL recommande de recourir à un prestataire exclusivement soumis au droit européen et offrant le niveau de protection adéquat. En France, pour les services d'informatique en nuage (ou *cloud* en anglais), la certification SecNumCloud de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) comprend ce critère et permet ainsi une protection des données contre les accès par des autorités étrangères.

Les lacunes et risques du projet de certification européenne EUCS

La possibilité de s'assurer, pour ces traitements les plus sensibles, que l'hébergeur des données n'est pas soumis à une législation extra-européenne ne figure plus dans le projet de certification européenne de cybersécurité du *cloud* EUCS piloté par l'Agence de l'Union européenne pour la cybersécurité (ENISA),

même dans les niveaux de certification les plus élevés, et même à titre optionnel.

Cette évolution, qui doit être rediscutée dès que la nouvelle Commission européenne aura été constituée, prive les acteurs d'un cadre concret pour garantir la protection des droits et libertés fondamentaux pour les citoyens européens dans le cadre de tels traitements.

En France, **la CNIL recommande depuis longtemps**, pour les bases de données personnelles les plus sensibles (telles que le système national des données de santé (SNDS) ou les données qui concernent des mineurs), d'assurer une protection contre les possibilités de divulgation à des autorités publiques de pays tiers. La CNIL a exprimé cette préoccupation à de nombreuses reprises.

Par ailleurs, **l'absence de niveau incluant des critères « d'immunité » pose problème sur le plan juridique, économique, technologique et industriel :**

- Elle **ne permet pas de stimuler l'offre européenne en matière de *cloud***, qui constitue le moyen technique de répondre aux besoins de développement et déploiement des systèmes d'intelligence artificielle. Elle n'offre pas non plus les moyens de faciliter l'accès à la commande publique pour les offreurs européens, là où les acteurs dominants actuels en ont pleinement bénéficié dans leur pays d'origine (en particulier via le programme FedRAMP aux États-Unis).

- Elle ne permet pas aux acteurs publics et privés de s'appuyer sur la certification EUCS pour externaliser dans le *cloud* leurs projets les plus sensibles, à l'image de ce que prévoit **la doctrine « *Cloud* au centre » de l'État français pour les administrations**. Celle-ci demande en effet aux autorités publiques de s'assurer que les données « *d'une sensibilité particulière* » hébergées dans le *cloud* ne soient pas soumises à des lois extra-européennes pouvant impliquer des injonctions de communication.

À noter : la loi française du 21 mai dernier visant à sécuriser et à réguler l'espace numérique (dite **loi SREN**) prévoit qu'en cas de recours à un service *cloud* par un prestataire privé **pour la mise en œuvre de systèmes informatiques traitant de données d'une sensibilité particulière pour l'État**, le service *cloud* doit mettre en œuvre des critères de sécurité et de protection des données afin d'empêcher **tout accès aux données par des autorités publiques d'États tiers** non autorisé par le droit de l'Union européenne ou d'un État membre de l'UE.

Pour toutes ces raisons, la CNIL appelle à l'inclusion, à titre optionnel, de critères « d'immunité » aux lois extra-européennes, qui peuvent s'inspirer de ceux de la qualification SecNumCloud déjà en place en France, dans le schéma de certification européen EUCS afin d'assurer la plus haute protection des traitements de données personnelles les plus sensibles pour les acteurs industriels européens.

Pour approfondir

- Présentation de l'EUCS
- La certification SecNumCloud pour les fournisseurs de services Cloud