Point sur

La souveraineté numérique

CME du 5 novembre 2024

DSN / DPO

31 octobre 2024

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Synthèse – La souveraineté numérique à l'AP-HP

Contexte et risques :

- Risques liés à l'utilisation de services numériques extra-européens
- Accès non autorisé aux données, réutilisation illégale, dépendance technologique, appauvrissement de l'industrie européenne

Enjeux du *cloud* souverain :

- Préserver l'indépendance technologique de l'UE
- Protéger les donnée sensibles contre la surveillance étrangère
- Recours à des prestataires européens conformes (*SecNumCloud*)

Réglementation et doctrine AP-HP :

- Textes et décisions européennes et françaises ;
- Doctrine AP-HP (2022) : *cloud* souverain pour les données sensibles (santé, recherche) avec exceptions possibles mais encadrées (engagement de migration notamment)

Prochaines étapes :

- Mise à jour de la doctrine d'ici mi-2025
- FAQ et documents explicatifs pour les professionnels AP et industriels
- Suivi rigoureux des engagements contractuels déjà conclus

1. Contexte et risques

- **L'utilisation des services de sociétés de services numériques (logiciel, hébergement, etc.) est nécessaire pour l'AP-HP, mais elle peut faire peser des risques, en particulier quand ces sociétés sont extra-européennes :**
  - Risque d'accès aux données des patients et des professionnels (ex. : demandes d'accès par des autorités judiciaires et/ou policières d'un autre État), notamment quand la société est soumise à un droit extra-européen.
  - Risque de réutilisation à des finalités interdites (ex. : revente / transfert de données à d'autres destinataires sans l'autorisation du responsable de traitement) ou de changements autoritaires des conditions d'utilisation avec des impacts sur les données
  - Risque de dépendance (*vendor lock-in*) vis-à-vis de grands industriels internationaux, dont nous serions une très petite fraction du chiffre d'affaires et à grande distance des décideurs, avec un faible pouvoir d'influence pour pouvoir peser lorsque c'est nécessaire (orientations stratégiques des produits, augmentations tarifaires radicales, rachat de l'entreprise, etc.)
  - Risque d'appauvrissement de l'industrie européenne si une partie substantielle de la valeur ajoutée (emplois, compétences, etc.) est transférée/maintenue dans d'autres pays

- **La souveraineté, c'est essayer de rester maître de ses choix de demain, en appliquant un ensemble de mesures de réduction de ces risques (choix des industriels, mesures contractuelles, mesures techniques) dans une approche pragmatique, en considérant les situations où la réelle absence d'alternative nous impose de devoir faire des exceptions.**

Le sujet se pose en particulier sur **l'hébergement des données en nuage** (*cloud*), où le prestataire a un accès très facile aux données. Le *cloud* est encore très peu utilisé à l'AP-HP, qui auto-héberge la majorité de ses SI, mais son usage se pose dans plusieurs projets émergents (nouveaux services numériques, recherche, etc.).

3. Définition et enjeux du *cloud* souverain

- **Définition** : hébergement des données effectué (i) par un hébergeur français ou UE et (ii) sur le sol français ou d'un État UE
- **Objectif** : garantir la sécurité et la confidentialité des données sensibles des citoyens de l'UE, en assurant que l'infrastructure *cloud* est sujette exclusivement aux réglementations protectrices applicables au sein de l'UE et protégée contre les décisions de nations étrangères
- **Application** : secteurs sensibles tels que la santé, dans lequel la protection des données est une priorité majeure (droit à la vie privée)
- **Origine** : risques d'accès illégaux aux données, affaire Snowden, lois de surveillance US extraterritoriales (même si les serveurs sont en UE, risque de transfert de données hors UE et accès à ces données par les autorités publiques US à l'insu des organismes concernés)

La plupart des **professionnels de santé** et des **patients** sont **très sensibles à ces enjeux** de confidentialité des données

Enjeux

Préservation de l'indépendance technologique de l'UE

Stimulation de l'économie de l'UE, renforcement de la compétitivité des entreprises de l'UE

Protection contre les risques d'espionnage, d'ingérence ou de surveillance massive

Lutter contre la dépendance des sociétés UE aux GAFAM (captivité/coût)

✓

OVHcloud

OUTSCALE

odrive

X

aws

Azure

iCloud

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

4. Contexte réglementaire et politique mouvant autour du *cloud* souverain

CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

La présidente

ASSISTANCE PUBLIQUE HOPITAUX DE PARIS
A l'attention de Mme Donatienne BLIN
55 BD DIDEROT
75012 PARIS 12

Lettre recommandée avec AR
N°AR : 2C 151 961 5730 8

Paris, le 17 MAI 2024

Instruction du dossier :
SANLAVILLE Claudine
N/Réf. : CSE/MED241051
Saisine N°P44-39311
(à rappeler dans toute correspondance)
Décision de mise en demeure n° 2024-062

- Au niveau européen, le RGPD prévoit des « **pays à protection équivalente** » vers lesquels il est possible d'envisager un transfert (ou de tolérer un « risque » de transfert). La commission européenne en est à son **3ème accord d'adéquation EU-USA (juillet 2023)**, après 2 accords cassés par la CJUE (2015 puis 2020), et un recours en cours sur le 3ème (par Schrems / NOYB). L'incertitude juridique est donc très élevée. L'article 32 du RGPD prévoit que le responsable de traitement met en œuvre les mesures pour garantir la sécurité.

- En France, **la circulaire Premier Ministre « *cloud* au centre »** de 2021 (mis à jour en 2023) s'applique à l'État et ses opérateurs (hôpitaux *a priori* non concernés). Elle impose (i) **recours au *cloud*** pour les nouveaux projets et (ii) **utilisation d'un *cloud* souverain SecNumCloud (SNC)** [référentiel ANSSI de 2022, avec des exigences de souveraineté très fortes (% du capital EU, localisation siège social, etc.)]

- **Certification EUCS** (*EU Cybersecurity Certification Scheme for Cloud Services*) en cours de travail au niveau européen, qui créerait un équivalent européen de la certification SNC. La CNIL a appelé à rehausser le niveau de protection des données dans ce projet de texte, face aux risques d'accès par une puissance étrangère.

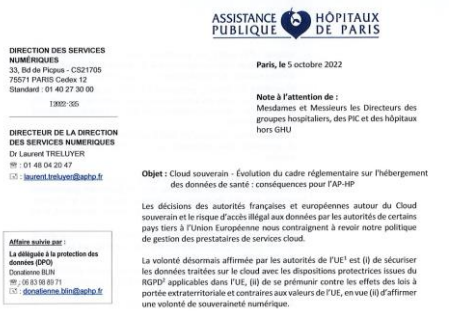
- Mail de la CNIL à l'AP-HP en juillet 2022 demandant de « **ne pas conclure de nouveaux contrats qui exposeraient des bases de santé à des lois étrangères** »

- **Mise en demeure de l'AP-HP par la CNIL le 17 mai 2024** sur un défaut d'encadrement du transfert de données vers les USA sur certaines briques logicielles de sécurité à l'AP-HP

- Renforcement de la souveraineté avec la **nouvelle version de la certification à l'hébergement des données de santé** (HDS) : localisation EU + transparence accrue, avec trajectoire de renforcement annoncée

- **Loi sécuriser et réguler l'espace numérique [SREN]** du 21 mai 2024 imposant, pour les traitements de données sensibles, à garantir contre tout accès par des autorités d'États tiers non autorisés par l'UE. Ce texte va par exemple désormais imposer à la plateforme des données de santé à sortir de Microsoft.

5. La doctrine AP-HP sur le *cloud* souverain d'octobre 2022



DIRECTION DES SERVICES NUMÉRIQUES
33, Bd de Picpus - CS21705
75571 PARIS Cedex 12
Standard : 01 40 27 30 00

DIRECTEUR DE LA DIRECTION DES SERVICES NUMERIQUES
Dr Laurent TREILUYER
☎ : 01 48 04 20 47
✉ : laurent.treiluyer@aphp.fr

Affaire suivie par :
La déléguée à la protection des données (DPO)
Donalienne BLIN
☎ : 06 83 98 89 71
✉ : donalienne.blin@aphp.fr

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Paris, le 5 octobre 2022

Note à l'attention de :
Mesdames et Messieurs les Directeurs des groupes hospitaliers, des PIC et des hôpitaux hors GHU

Objet : Cloud souverain - Évolution du cadre réglementaire sur l'hébergement des données de santé : conséquences pour l'AP-HP

Les décisions des autorités françaises et européennes autour du Cloud souverain et le risque d'accès illégal aux données par les autorités de certains pays tiers à l'Union Européenne nous contraignent à revoir notre politique de gestion des prestataires de services cloud.

La volonté désormais affirmée par les autorités de l'UE[1] est (i) de sécuriser les données traitées sur le cloud avec les dispositions protectrices issues du RGPD[2] applicables dans l'UE, (ii) de se prémunir contre les effets des lois à portée extraterritoriale et contraires aux valeurs de l'UE, en vue (ii) d'affirmer une volonté de souveraineté numérique.

- **Doctrine AP-HP sur le *cloud* souverain définie en octobre 2022**, pour garantir la confidentialité des données médicales, qui va, par choix, plus loin que le strict cadre réglementaire
- **<u>Principe</u> : pour l'hébergement *cloud* des données de santé, recherche ou soin (services numériques, dispositifs médicaux numériques, objets connectés, etc.), recours par principe aux *clouders* souverains**, c'est-à-dire ceux garantissant leur conformité au référentiel SecNumCloud de l'ANSSI (= une petite dizaine de fournisseurs actuellement, ou équivalent européen) et donc leur immunité contre les lois ou décisions extra-européennes.
- **Des exceptions** :
  - Niveau 1 : si le prestataire est européen, que l'hébergement est physiquement localisé en UE et que le partenaire **s'engage à migrer vers une solution conforme dans les 24 ou 36 mois**
  - Niveau 2 : à défaut, s'il n'y a **pas d'alternatives raisonnables** (ex. : monopole, etc.) ou si le **projet est jugé particulièrement stratégique**, avec une balance bénéfice/risque acceptable pour les patients – alors une exception peut être effectuée par le représentant du responsable de traitement AP-HP, en privilégiant la collégialité et en traçant la décision au registre RGPD de l'AP-HP sur le traitement concerné

6. Bilan sur la doctrine AP-HP sur le *cloud* souverain (1/2)

Aspects positifs :

- ✓ Sécurisation des contrats pour l'avenir compte tenu de l'instabilité / des évolutions règlementaires (garanties contractuelles anticipées par l'AP-HP, déjà inscrites au contrat si jamais la décision d'adéquation CE est encore annulée)
- ✓ Une application pragmatique, avec pédagogie et souplesse, ayant conduit à très peu de situations difficiles
- ✓ Une conviction des entreprises du numérique en santé, d'aller, au moins pour certains usages, sur de l'hébergement souverain, avec de multiples partenaires qui se sont engagés (Doctolib, Lifen, Philips, Dassault, Nabla, Satelia, Predict4health - migration récemment effectuée pour ces 2 derniers - etc.)
- ✓ Des patients et professionnels rassurés par la doctrine de l'AP-HP
- ✓ Une sensibilisation forte des professionnels de l'AP-HP sur ces enjeux
- ✓ D'autres hôpitaux français qui ont initié cette approche

7. Bilan sur la doctrine AP-HP sur le *cloud* souverain (2/2)

Difficultés :

- Des partenaires parfois arcboutés contre cette exigence aux motifs (i) que les *clouds* européens sont trop chers, pas encore assez développés en termes techniques, (ii) qu'ils sont captifs de leurs prestataires de *clouds* américains (triade AWS/GCP/Azure) et (iii) qu'ils sont des entreprises mondiales, qui ne veulent pas adapter leurs pratiques pour leurs clients européens
- L'action coercitive de l'AP-HP est parfois très limitée auprès de certains grands acteurs internationaux, avec des négociations parfois compliquées ou impossibles. Ex. : Abott / Medtronic / Cochlear, etc. dont les dispositifs sont parfois déjà implantés…
- Absence de visibilité sur l'exhaustivité des traitements au sein de l'AP-HP impliquant des hébergements sur des prestataires non souverains et hors UE
- *Contract management* rigoureux à mener par DPO / directions responsables sur les contrats conclus intégrant l'engagement de migration et suivi/retour/relance auprès des partenaires du respect de l'engagement
- Encore trop faible lisibilité de la démarche avec certains acteurs qui résument par facilité « le RGPD ça bloque nos activités »

8. Prochaines étapes proposées

Face à un contexte évolutif…

- Régulations nouvelles au niveau UE (EUCS) et FR (SREN), le risque d'un 3ème arrêt CJUE contre la décision d'adéquation UE-USA
- Amélioration de l'offre de *cloud* européenne (démonstrateur DINUM en France, etc.)

… maintenir cette doctrine, face aux enjeux de protection des données et de souveraineté, en :

- Expliquant mieux sont contenu et notamment les conditions d'exception, notamment en :
  - Mettant à jour la doctrine, avant mi-2025, pour en améliorer la lisibilité
  - Rédigeant et en publiant une FAQ pratique à destination des professionnels de l'AP-HP
  - Rédiger une fiche pratique à destination des industriels leur expliquant la doctrine
- Incitant nos partenaires industriels à rentrer dans la démarche, tout en maintenant une pratique des dérogations (niveau 1 et 2), mieux présentées à la collégialité (codir DG pour des sujets stratégiques, COPIL données pour la réutilisation secondaire, points semestriels sur les enjeux DPO, niveau de directions fonctionnelles / des GHU, etc.), avec traçabilité associée dans le registre AP-HP des traitements de données pour les contrôles CNIL (outil Dastra)