BSA - The Software Alliance

Commission européenne – Notification 2023/0632/FR (France)

PJL SREN - Position sur les critères de souveraineté (Art. 10 bis et 10 bis A)

Dans le cadre de la procédure de notification 2023/0632/FR à la Commission européenne par le gouvernement français, concernant le projet de loi visant à sécuriser et réguler l'espace numérique (PJL SREN), BSA souhaite attirer l'attention de la Commission européenne sur certains articles du projet de loi dans sa version issue de l'Assemblée nationale.

BSA souhaite mettre en avant le fait que ces articles spécifiques (10 bis et 10 bis A), de même que l'ensemble du Titre III relatif à l'informatique en nuage dont beaucoup visent *a minima* à anticiper le Data Act, n'ont pas été notifiés à la Commission européenne dans leur dernière rédaction, alors même que nous estimons qu'ils engendrent une triple inadéquation :

1. Une inadéquation juridique avec le droit européen ;
2. Une inadéquation pratique en termes de cybersécurité et de protection des données ;
3. Une inadéquation économique générant des risques significatifs sur l'économie et la sécurité des données en France et en Europe.

I. Une inadéquation juridique avec le droit européen

De prime abord, sur le plan juridique, ces articles, et le contenu qu'ils visent, ne figurent nullement dans le Règlement européen relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (Règlement sur les Marchés Numériques ou « DMA ») ni dans le Règlement européen fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (Règlement sur les Données ou « Data Act ») qui devrait entrer en vigueur d'ici la fin d'année 2023.

Afin d'éviter une profonde incohérence entre le droit européen et français, nous estimons nécessaire une réécriture qui prendrait en considération l'adéquation de ces articles avec le droit communautaire existant.

II. Une inadéquation pratique en termes de cybersécurité et de protection des données

Ces articles visent à mettre en avant une vision "politique" et "souveraine" de la cybersécurité en général, et de la protection des données plus spécifiquement, au contraire d'une approche centrée sur la dimension technique, portée au niveau européen. Si la version de l'Assemblée nationale nuance le travail mené au préalable par le Sénat, force est de constater que la philosophie de ces articles n'a pas évolué.

En effet, l**es articles 10 bis A et 10 bis ajoutent des critères dits de « souveraineté »** (à savoir des critères qui seront définis par décret et intègreront des exigences relatives à la "détention capitalistique" et qui concernent les services d'informatiques en nuage contractés par "les administrations de l'État ou ses opérateurs, dont la liste est annexée au projet de loi de finances") pour toute offre commerciale sur le marché de l'informatique en nuage pour l'hébergement ou le traitement :

- des données qui relèvent de secrets protégés par la loi au titre des articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration ;
- aux données nécessaires à l'accomplissement des missions essentielles de l'État, notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes.

Cette approche devrait également s'appliquer prochainement, via l'article 10 bis B du même projet de loi SREN, aux données de santé à caractère personnel mentionnées à l'article L. 1111-8 du code de la santé publique, ainsi qu'aux données d'archivage. Le gouvernement a, en effet, annoncé une révision de son référentiel HDS (Hébergement des Données de Santé), notifié à la Commission européenne le 5 décembre 2023) qui pourrait inclure des critères de souveraineté. Les données d'archivage sont, quant à elles, soumises à une obligation de localisation des données indépendamment de l'évolution dudit référentiel.

Ces critères de « souveraineté » imposent aux entreprises des obligations de plusieurs natures. Ainsi, une garantie de "protection des données traitées ou stockées contre tout accès non autorisé par des autorités publiques d'États en dehors de l'Union européenne" sera nécessaire. Mais surtout, l'article 10 bis A spécifie que la détention capitalistique sera considérée dans le cadre d'un décret en Conseil d'Etat, incluant de fait un critère capitalistique dont l'étendue reste incertaine.

Ces critères exorbitants oublient que l'objectif principal de la (cyber)sécurité, comme de la protection des données, est avant tout la sécurité et la protection. En ce sens, les obligations visant à garantir la sécurité et la protection des données doivent donc être – par nature – techniques, technologiquement neutre, fondées sur une approche des risques et viser des fonctionnalités ou résultats pratiques et concrets. De plus, l'article 10 bis A apparaît d'autant plus prématuré en raison d'une part, du fait qu'il n'existe à ce jour **aucun consensus européen sur les règles nécessaires** (en particulier, les exigences du niveau 3 du futur schéma de certification européen sur les services en nuage – EUCS – restent à déterminer) et d'autre part, en raison de l'**indisponibilité sur le marché français et européen d'offres commerciales susceptibles de répondre aux exigences de souveraineté envisagées**. A ce titre, il faut relever que, partant de ce constant, la Feuille de route[1] du numérique en santé 2023-2027 prévoit, concernant le traitement des données de santé, que de nouvelles exigences en termes de souveraineté ne soient envisagées qu'à l'horizon 2027.

III. Une inadéquation économique générant des risques significatifs sur l'économie et la sécurité des données en France et en Europe

L'ajout de ces critères de « souveraineté » pour garantir la (cyber)sécurité et la protection des données induit des risques majeurs, sous-estimés dans la version actuelle du texte :

1. **La création d'importantes barrières à l'entrée d'entreprises non-établies sur le territoire de l'UE ou d'entreprises opérant ou investissant sur la scène internationale**. Cela limiterait la concurrence sur le marché de l'informatique en nuage, augmenterait le coût des services d'informatique en nuage et limiterait drastiquement le choix de partenaires technologiques de confiance pour les entreprises européennes.

2. **L'atteinte à la coopération internationale sur le partage d'informations et la détection des menaces de cybersécurité et de vulnérabilités**, comme le fait de travailler à des solutions communes pour répondre à la cyber-résilience dans l'environnement géopolitique actuel. La nécessité de partenariats avec des pays alliés pour protéger et sécuriser les données sensibles, et de localiser les données dans des lieux différents, notamment en dehors de son territoire apparaît plus que jamais pertinente.

3. **La fin de la possibilité pour la grande majorité des entreprises d'informatique en nuage non-européennes d'offrir leurs services à leurs clients établis sur le territoire de l'UE.** Cette situation ralentirait considérablement le processus de transformation numérique en cours, promu par le Gouvernement français et la Commission européenne. En effet, face à l'incertitude liée à ces critères de « souveraineté », les entreprises et certaines administrations publiques françaises et européennes, clientes d'entreprises non-européennes, gèlent, à ce stade, plusieurs contrats de services d'informatique en nuage.

[1] https://participez.esante.gouv.fr/project/feuille-de-route-du-numerique-en-sante-2023-2027/presentation/presentation

4. **Une incitation pour d'autres juridictions d'introduire des critères ou obligations similaires.** En effet, plusieurs pays, notamment les Etats-Unis, dont le régime FedRAMP (Federal Risk and Authorization Management Program) actuel concerne les aspects techniques de la cybersécurité de l'informatique en nuage sans toutefois imposer des mesures de « souveraineté » équivalentes, pourrait être adapté pour inclure des critères de capitalisation et, de ce fait, contribuerait à augmenter la fragmentation dans les solutions de cybersécurité parmi des pays partenaires.

5. **Un frein à l'expansion des opportunités des entreprises européennes sur les marchés non-européens.** De fait, les critères de « souveraineté », comme d'immunité à la législation non-européenne, s'appliquera également, aux entreprises européennes, impactant leur accès aux marchés non-européens.