COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2024-05 DU 4 SEPTEMBRE 2024
SUR LES ENJEUX POLITIQUES ET ECONOMIQUES DU SCHEMA EUROPEEN DE CERTIFICATION DE SECURITE DES SERVICES CLOUD

Les membres de la Commission supérieure du numérique et des postes (CSNP) souhaitent attirer l'attention des pouvoirs publics et celle des membres de la représentation nationale sur les enjeux politiques et économiques du schéma européen de certification de sécurité des services cloud (EUCS) et formuler des recommandations pour renforcer la protection des données sensibles, à caractère personnel ou non, de nos concitoyens, de nos entreprises et de nos administrations publiques.

En effet, alors que la Commission nationale de l'information et des libertés (CNIL) vient de s'exprimer sur les lacunes et risques du projet de certification européenne EUCS[1] et qu'un nouvel exécutif se met en place au niveau européen, il est essentiel que ces enjeux de souveraineté soient portés au plus haut niveau.

Il est également important de rappeler que la sécurité numérique repose sur trois principes :

- intégrité des systèmes d'information, des données et des traitements associés ;
- disponibilité des systèmes d'information et des données ;
- confidentialité des données et des traitements associés.

La confidentialité des données et des traitements associés consiste à s'affranchir de deux types de menaces majeures, mais bien distinctes :

- les accès illégitimes et illégaux, de nature criminelle, qu'ils soient le fait d'organisations criminelles ou d'agences étatiques ;
- les accès par des agences de renseignement qui agissent dans un cadre légal mais secret, et bien entendu illégitimes pour les organismes qui en sont les victimes.

De nombreux opposants à toute forme de protection contre les accès légaux aux données détenus par les opérateurs de services cloud, entretiennent à dessein une confusion sur la confidentialité entre les enjeux de cybersécurité contre les accès illégitimes et illégaux aux données sensibles et stratégiques des européens et les dispositions de protection des données

[1] Cloud : les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles | CNIL

sensibles et stratégiques contre ces accès légaux. Ces dispositions sont en effet mises en œuvre par les agences de renseignement pour tout type d'activité, notamment pour mener des activités d'intelligence économique au profit de leurs entreprises et au détriment des entreprises des concurrents économiques.

I. Genèse du schéma européen de certification des services cloud (EUCS)

Face à l'expansion rapide des services cloud et à leur adoption croissante par les entreprises et les administrations publiques, l'Union Européenne a jugé nécessaire d'instaurer un cadre réglementaire pour assurer la sécurité et la conformité de ces services sur le marché européen. Cette initiative a conduit à la création du Schéma Européen de Certification des Services Cloud (EUCS). L'objectif de ce schéma est de renforcer la confiance des utilisateurs dans les services cloud en garantissant un haut niveau de sécurité, de protection des données, et de conformité aux lois européennes.

Le projet EUCS s'inscrit dans la stratégie plus large de l'Union Européenne visant à construire un marché numérique résilient et sécurisé. L'adoption du **Règlement 2019/881**, dénommé **Cybersecurity Act**, a posé les bases d'un cadre commun pour la certification en matière de cybersécurité. L'Agence de l'Union Européenne pour la Cybersécurité (ENISA) a été mandatée pour développer et gérer différents schémas de certification, parmi lesquels l'EUCS occupe une place centrale. L'EUCS a pour ambition de fournir un cadre juridique homogène au sein de l'Union, non seulement pour protéger les données sensibles, qu'elles soient personnelles ou non, mais aussi pour renforcer la souveraineté numérique de l'Europe face à la concurrence mondiale.

II. L'arrêt de la CJUE invalidant le Privacy Shield et ses implications

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE)[2] a rendu un arrêt crucial qui a invalidé le Privacy Shield, un accord régissant le transfert des données à caractère personnel entre l'Union Européenne et les États-Unis. Cet arrêt a mis en lumière les pratiques des agences de renseignement américaines, qui accèdent aux données personnelles des citoyens européens via des fournisseurs de services cloud américains. Ces données, lorsqu'elles sont hébergées par des prestataires américains, sont soumises à des législations, notamment **la section 702 du Foreign Intelligence Surveillance Act (FISA)**, qui permettent aux États-Unis de collecter des données, de façon massive, à priori, et sans mandat judiciaire, sans offrir les garanties de proportionnalité exigées par le droit de l'Union Européenne. Le considérant 184 de cet arrêt souligne que ces législations ne respectent pas les garanties minimales requises par l'Union, car les programmes de surveillance qui en découlent ne sont pas limités à ce qui est strictement nécessaire.

[2] Arrêt C-311/18 du 16 juillet 2020 Data Protection Commissioner contre Facebook Ireland Ltd/ Maximillian Schrems EUR-Lex - 62018CJ0311 - EN - EUR-Lex (europa.eu)

En invalidant le Privacy Shield, la CJUE a principalement mis en avant la protection des données à caractère personnel. Toutefois, la section 702 de la FISA ne se limite pas aux données personnelles et s'étend également aux données non personnelles, et permet l'accès à tout type de données sensibles ou stratégiques. Cela exacerbe les préoccupations concernant la sécurité des informations économiques européennes.

Le Data Privacy Framework (DPF), adopté en juillet 2023 pour remplacer le Privacy Shield, ne couvre l'adéquation des transferts vers les États-Unis que pour les données à caractère personnel. En revanche, la protection des données non personnelles sensibles ou stratégiques vis-à-vis des activités des agences de renseignement fait toujours face à un vide juridique au sein de l'Union européenne.

Ce cadre lacunaire souligne la nécessité d'une distinction claire entre les besoins légitimes des États-Unis en matière de lutte contre le terrorisme et le crime international, et les risques que peuvent engendrer les activités abusives d'intelligence économique à l'encontre des entreprises européennes visant à avantager leur économie. Par ailleurs, un risque majeur persiste, constitué par la différence d'interprétation des principes de proportionnalité et de nécessité entre l'Union européenne et les États-Unis. Ces principes sont au cœur des garanties apportées par le DPF (Data Privacy Framework), mais leur application dépend largement du contexte juridique et culturel de chaque juridiction. En Europe, la protection des données personnelles est un droit fondamental strictement encadré, et toute limitation de ce droit doit être nécessaire, proportionnée et justifiée de manière rigoureuse.

Les autorités européennes, y compris la CJUE, interprètent ces principes dans un cadre où les droits individuels priment, même face à des enjeux de sécurité. Aux États-Unis, ces mêmes principes sont interprétés dans un contexte où la sécurité nationale occupe une place prépondérante. Le cadre juridique américain, notamment sous la section 702 du Foreign Intelligence Surveillance Act (FISA), autorise une surveillance extensive des personnes (physiques ou morales) étrangères pour des motifs de sécurité nationale, ce qui peut inclure la collecte massive de données.

Malgré les réformes introduites par le décret présidentiel 14086, adopté par le Président Biden pour permettre la mise en œuvre du DPF, et qui visent à renforcer les protections dont bénéficient les données à caractère personnel des européens, le concept de « nécessité » aux États-Unis peut inclure des actions que les autorités européennes pourraient juger excessives. Cette divergence d'interprétation pourrait devenir une source de tensions à l'avenir.

Si les autorités européennes estiment que les principes de proportionnalité et de nécessité ne sont pas appliqués selon les standards du RGPD, elles pourraient contester la validité du Data Privacy Framework. Un tel désaccord pourrait entraîner une nouvelle invalidation de l'accord, comme ce fut le cas pour le Privacy Shield. Ce risque met en lumière les défis inhérents à l'harmonisation des normes de protection des données entre deux systèmes juridiques qui, bien que partenaires, sont fondamentalement différents.

III. Le cadre de labellisation de Gaia-X

En novembre 2021, l'association Gaia-X a adopté un cadre de certification pour les services cloud, organisé autour de trois niveaux de labellisation. Le niveau le plus élevé de ce cadre inclut des exigences en matière d'immunité contre les législations non européennes à portée extraterritoriale. Ce consensus parmi les membres européens de Gaia-X reflète une volonté claire, tant des bénéficiaires de services cloud labellisés que des fournisseurs de ces services, de protéger les espaces de partage des données les plus sensibles contre les ingérences légales mais potentiellement abusives des législations étrangères.

IV. Le référentiel SecNumCloud et la loi SREN

Le référentiel SecNumCloud, élaboré par l'ANSSI en 2016, est un cadre de sécurité destiné à qualifier les prestataires de services cloud. Il s'appuie sur la norme ISO/IEC 27001 et répond aux exigences européennes, notamment en matière de protection des données, tout en garantissant un haut niveau de sécurité technique, opérationnelle et juridique. La version 3.2 du référentiel, publiée en 2022, renforce les protections contre les lois extra-européennes, conformément à l'arrêt « Schrems II » de la Cour de justice de l'Union européenne. Elle est par ailleurs cohérente avec les exigences du niveau High+ de la précédente version de l'EUCS.

Ce référentiel vise à créer un environnement cloud sécurisé, à encourager le développement d'acteurs nationaux des services cloud notamment pour répondre aux besoins de l'État, et à assurer une confiance durable entre les prestataires qualifiés et leurs utilisateurs, en particulier pour les administrations publiques qui gèrent des données sensibles. La certification SecNumCloud, matérialisée par le Visa de sécurité ANSSI, est un gage de fiabilité et de conformité aux normes de sécurité les plus élevées, offrant ainsi une protection accrue contre les cyberattaques et les risques juridiques.

L'incertitude juridique demeure, mais il est fort probable que l'adoption de l'EUCS, qu'il intègre ou non le niveau High+, rendrait caduque le référentiel SecNumCloud. Dans l'hypothèse de l'adoption par la Commission européenne d'un EUCS qui n'intègrerait pas des exigences d'immunité aux législations non européennes à portée extraterritoriale, et qui se substituerait en Europe à tous les autres référentiels nationaux de certification de services cloud, l'État français se trouverait démuni pour mettre en œuvre sa stratégie dite « cloud au centre ». Par ailleurs, dans une telle hypothèse, la mise en œuvre des articles 31 et 32, relatifs à la protection des données stratégiques et sensibles sur le marché de l'informatique en nuage, de la loi visant à sécuriser et à réguler l'espace numérique, dite loi SREN, du 21 mai 2024 serait difficile. Ces articles font, en effet, sans le nommer mais de manière transparente, référence au référentiel SecNumCloud.

V. Le niveau High+ de l'EUCS

C'est dans ce contexte, que la première version de l'EUCS a intégré dans son niveau de certification le plus élevé, également appelé **High+, des critères techniques et juridiques**

d'immunité des services cloud aux législations non européennes à portée extraterritoriale. Si de nombreux Etats disposent de ce genre de disposition légale, le niveau High+ vise en premier lieu les Etats dont dépendent les principaux opérateurs mondiaux de services cloud. La Chine dispose, avec sa loi du 28 juin 2017 sur le renseignement national, d'une disposition législative qui oblige les opérateurs cloud chinois comme Alibaba, Tencent ou Huawei, de mettre à la disposition des autorités chinoises les données dont elles peuvent disposer sur leurs infrastructures sans en référer à leurs clients. Le mécanisme est assez similaire à celui dont les Etats-Unis disposent avec la section 702 du FISA, mis en exergue par la CJUE, et auquel sont bien entendu soumis les principaux opérateurs de service cloud américain dont les trois principaux qui préemptent en Europe plus de 70% du marché des services cloud.

Ce niveau High+ a été conçu suivant des principes analogues à ceux du référentiel français SecNumCloud, afin d'offrir une protection proportionnée aux entreprises européennes traitant des données dans le cloud et risquant une appropriation illégitime via des voies légales non européennes à portée extraterritoriale. Cette protection, bien que non obligatoire, est jugée essentielle pour ces entreprises.

Il existe au sein de l'écosystème numérique européen, notamment au sein des organismes publics et privés qui expriment le besoin de services cloud immunisés contre les législations non européennes à portée extraterritoriale, un large consensus pour considérer que le niveau High+ est la clé de voûte des dispositifs européens de développement d'une industrie européenne autonome des services cloud. Sans ce dispositif, il sera extrêmement compliqué de sortir de cette situation de dépendance croissante vis-à-vis des opérateurs américains, qui pourrait à terme porter des risques insupportables de nature économique, géopolitique et juridique.

VI. Les critiques américaines

Cette initiative européenne a suscité de vives réactions aux États-Unis. Le 25 mai 2023, plusieurs associations professionnelles américaines, dont la Computer & Communications Industry Association (CCIA) et la Business Software Alliance (BSA), ont adressé une lettre à des membres clés de l'administration Biden, dénonçant le niveau High+ de l'EUCS comme une menace pour la sécurité nationale des États-Unis. Elles écrivent notamment dans ce courrier : « *EUCS is part of a broader concerted effort by Europe to enact a "digital sovereignty" agenda that seeks to disadvantage U.S. firms for the benefit of local alternatives,* ***potentially threatening U.S. economic and national security interests****.* » Selon eux, l'EUCS s'inscrit dans une démarche de «souveraineté numérique » européenne visant à désavantager les entreprises américaines, compromettant ainsi les intérêts économiques et sécuritaires des États-Unis.

En septembre 2023, le secrétaire d'État américain Antony Blinken a envoyé une note diplomatique à la présidente de la Commission européenne, Ursula von der Leyen, avertissant que l'inclusion de ces dispositions dans le schéma final pourrait nuire aux relations bilatérales entre les États-Unis et l'Union Européenne, tant sur le plan économique que sécuritaire : « *Including these provisions in the final scheme* ***could also negatively impact the U.S.-EU bilateral economic and security relationship****.* »

VII. Réactions européennes

En réaction, la Commission européenne a demandé à l'ENISA de revoir le schéma EUCS, ce qui a conduit à une proposition début 2024 d'un schéma expurgé du niveau High+, c'est-à-dire de toute disposition garantissant l'immunité contre les législations non européennes comme la section 702 du FISA. En avril 2024, le Congrès américain a renouvelé pour deux ans la section 702 du FISA, en élargissant par ailleurs son champ d'application.

Le 30 octobre 2023, lors d'un sommet ministériel entre l'Allemagne, la France et l'Italie, consacré à la coopération industrielle dans plusieurs secteurs stratégiques pour l'Union européenne, ces trois pays ont réaffirmé leur intention de renforcer la protection des données sensibles en Europe, en particulier contre les législations extraterritoriales. Cette volonté de protection a toutefois été remise en question, notamment par l'Allemagne, dans le cadre des discussions sur l'EUCS.

Pour de nombreuses entreprises européennes, le niveau de certification High+ de l'EUCS est crucial pour protéger de manière non contraignante leurs données non personnelles sensibles ou stratégiques contre les accès légaux mais indésirables des services de renseignement, notamment américains. Ces entreprises ne souhaitent pas une éviction des fournisseurs de services cloud américains du marché européen, mais affirment qu'une partie substantielle de leurs besoins ne peut être satisfaite par ces opérateurs. Elles insistent sur la nécessité de disposer en Europe de services cloud capables de répondre à leurs exigences de protection de leurs données sensibles et stratégiques, mis en œuvre de manière homogène sur l'ensemble du territoire de l'Union, avec une robustesse garantie par un schéma de certification européen à valeur légale.

Au sein de l'Union européenne, les opposants au niveau High+ de l'EUCS se retrouvent schématiquement dans deux grandes catégories :

- les Etats membres de l'Union Européenne sensibles aux menaces de restriction des garanties de sécurité que les Etats-Unis leur apporte ;
- les secteurs d'activité fortement dépendant du marché des Etats-Unis et sensibles aux menaces de restriction d'accès à ce marché en cas d'adoption du niveau High+ dans l'EUCS.

VIII. Conformité du niveau High+ aux accords de l'Organisation Mondiale du Commerce (OMC)

Une critique récurrente du niveau High+ de l'EUCS consiste à mettre en doute sa conformité aux engagements de l'Union européenne pris dans le cadre des accords de l'OMC, au motif qu'il provoquerait l'éviction des opérateurs américains de certains marchés. Dans un article publié le 1er septembre 2023 sur le site du *Center for Strategic and International Studies* (CSIS), organisme américain de recherche qui se consacre à la promotion d'idées pour relever les grands défis du monde, Meredith Broadbent développe une attaque en règle contre le niveau

High+ de l'EUCS, notamment en affirmant l'incompatibilité du niveau High+ avec les accords de l'OMC.

Cet argument ne tient pas car ce n'est pas le référentiel en lui-même qui pourrait être incompatible avec les termes des accords l'OMC, mais l'usage qui en sera éventuellement fait par les États membres, notamment dans le cadre des marchés publics pour garantir des conditions de concurrence ouvertes, équitables et transparentes, en réservant l'usage du niveau High+ aux cas dérogatoires explicitement prévus dans le traité.

D'ailleurs, l'Union européenne n'a pas prononcé de non-conformité du référentiel SecNumCloud aux accords de l'OMC. En revanche, la première circulaire du Premier Ministre sur la mise en œuvre de la stratégie « cloud au centre », publiée le 5 juillet 2021, a été critiquée par Bruxelles en raison de sa non-conformité aux accords de l'OMC. Elle a dû être actualisée en mai 2023, notamment pour tenir compte des observations de la Commission européenne.

IX. Position de la CNIL

Dans le contexte créé par les doutes sur la robustesse du DPF au regard de la protection des données personnelles les plus sensibles, la Commission Nationale de l'Informatique et des Libertés (CNIL), dans une position publiée le 19 juillet 2024, a critiqué les lacunes du projet actuel de certification EUCS, en particulier en ce qui concerne la protection des données personnelles sensibles contre les accès non autorisés par des autorités étrangères. La CNIL a souligné que l'absence de critères « d'immunité » contre les législations non européennes affaiblit la compétitivité de l'offre cloud européenne et compromet la capacité des acteurs publics et privés à externaliser leurs projets les plus critiques de manière sécurisée. Elle a appelé à réintroduire des dispositions inspirées du cadre SecNumCloud au sein de l'EUCS, permettant aux prestataires européens de cloud de démontrer leur capacité à protéger les données contre toute ingérence étrangère.

X. Les conclusions et recommandations de la CSNP

La Commission supérieure du Numérique et des Postes :

- considère que l'adoption du schéma de certification EUCS, incluant des dispositions garantissant l'immunité contre les législations non européennes, est un enjeu essentiel d'autonomie technologique pour l'Union européenne, la condition de l'émergence d'une industrie européenne des services cloud, et une impérieuse nécessité pour protéger les données sensibles et stratégiques, à caractère personnel ou non, des organismes publics et privés qui ont besoin de préserver leur patrimoine informationnel contre les ingérences étrangères ;

- demande au Gouvernement de présenter à la Représentation nationale l'état des négociations et de lui préciser sa position et son évolution au cours de celle-ci ;

– invite le Gouvernement à solliciter la Commission européenne pour que celle-ci confirme le caractère volontaire d'usage des différents niveaux de certification de l'EUCS par les bénéficiaires des services cloud certifiés ;

– suggère au Gouvernement de demander aux différents États membres de l'UE, opposés au niveau High+, de s'expliquer sur les raisons pour lesquelles ils entendent en priver les entreprises et les administrations publiques qui en expriment le besoin en Europe ou dans leur propre pays ;

– demande au Gouvernement de faire le nécessaire auprès de la Commission européenne pour qu'elle sursoit à toute décision d'adoption de la version actuelle du schéma de certification afin qu'un travail approfondi de prise en compte de tous les besoins puisse être mené avec les différentes parties prenantes, notamment les organisations professionnelles européennes représentatives des potentiels futurs bénéficiaires, publics et privés, de l'EUCS ;

– demande au Gouvernement de mener une analyse approfondie des conséquences géopolitiques à moyen terme des renoncements de l'Union européenne à maintenir dans l'EUCS un niveau de type High+ ;

– demande au Gouvernement de mener une analyse économique sur les conséquences des dépendances européennes à l'industrie américaine des services cloud et sur son impact sur la compétitivité de l'économie européenne ;

– demande au Gouvernement de lui présenter une analyse des risques que l'adoption du niveau High+ dans l'EUCS ferait peser sur l'Union européenne au titre des engagements de celle-ci dans le cadre des accords de l'OMC.