Les **Briefings France-Allemagne** du cep

LES TRANSFERTS ILLÉGAUX DE DONNÉES VERS LES ÉTATS-UNIS

ÉLÉMENTS CLÉS

L'arrêt « Schrems II » de la CJUE

- Les transferts de données personnelles de l'UE vers les États-Unis ne peuvent plus être fondés sur la décision d'adéquation « Privacy Shield » de la Commission européenne. La Cour de justice de l'Union européenne (CJUE) a déclaré à juste titre cette décision invalide dans l'arrêt « Schrems II » parce que le « bouclier de protection des données UE-États-Unis » (ou « Privacy Shield ») n'offrait pas une protection des données équivalente à celle garantie au sein de l'UE.
- Les transferts de données vers un pays tiers sur la base de clauses contractuelles types (CCT) – c'est-à-dire des clauses types de protection des données adoptées par la Commission européenne et convenues entre l'exportateur et le destinataire des données – sont toujours autorisés sur le principe. Toutefois, les exportateurs comme les destinataires de données doivent vérifier que la législation du pays tiers et les CCT assurent, dans leur ensemble, un niveau de protection des données substantiellement équivalent à celui qui est garanti au sein de l'UE, et que les personnes concernées dont les données sont transférées disposent de droits opposables et de voies de droit effectives.

L'exécution de l'arrêt « Schrems II »

- Le Comité Européen de la Protection des Données (CEPD) a publié deux projets de recommandations suite à cet arrêt. Selon ces projets, toutes les circonstances du transfert de données spécifiques – y compris les catégories et le format des données transférées – doivent être prises en compte lors de l'examen du niveau de protection des données dans le pays tiers, mais pas l'évaluation subjective de la probabilité d'accès par les autorités.
- En outre, selon les CCT, l'exportateur et le destinataire des données doivent vérifier si le droit du pays tiers permet également au destinataire des données de respecter les CCT. Ce qui est problématique, ce sont en particulier les transferts de données à des destinataires auxquels le droit du pays tiers impose des obligations contraires aux CCT et qui portent atteinte à leur garantie.
- Selon le CEPD, l'obligation du destinataire des données de divulguer ou de permettre aux autorités du pays tiers d'accéder à ces données ne va pas à l'encontre du respect des CCT si le pays tiers respecte les « garanties européennes essentielles » dans ses activités de contrôle.
- Les mesures de surveillance respectent les « garanties essentielles européennes » du CEPD si elles sont basées sur des règles claires pour le traitement des données, si les interventions sont nécessaires et proportionnées, et si un contrôle indépendant et des voies de droit effectives existent dans le pays tiers.
- Si les mesures de surveillance ne sont pas conformes aux garanties essentielles européennes – ce qui est le cas des lois américaines de surveillance – , il manquera un niveau de protection substantiellement équivalent à celui qui est garanti au sein de l'UE. Les CCT ne suffisent pas à elles-seules ; l'exportateur de données doit plutôt prévoir des mesures supplémentaires de protection des données.
- Il existe une insécurité juridique quant aux mesures supplémentaires que l'exportateur de données doit prendre pour combler les lacunes en terme de protection. À cette fin, les autorités de contrôle proposent des mesures techniques telles que l'anonymisation, le cryptage, la pseudonymisation ou le fractionnement des données, l'insertion de clauses contractuelles complémentaires et de mesures organisationnelles.
- Imposer au destinataire et à l'exporteur des données des obligations contractuelles plus strictes – telles que l'obligation d'informer sur les accès aux données ou la possibilité de les contester juridiquement – et introduire des mesures organisationnelles – telles que les lignes directrices internes des entreprises – permettent d'augmenter le niveau de protection des données, mais de telles mesures ne se suffisent pas à elles seules et doivent être complétées par des mesures techniques. En effet, même des obligations contractuelles renforcées ne peuvent ni lier les autorités du pays tiers ni créer des voies de droit effectives pour les citoyens de l'UE.

L'auteure : Anja Hoffmann | hoffmann@cep.eu
Centre de Politique Européenne | 18 rue Balard | 75015 Paris | France | Téléphone : + 33 (0)1 45 54 91 | www.cepfrance.eu/fr
D'après l'étude originale: Unzulässigkeit der Datenübermittlung in die USA.
Briefing préparé par Marion Jousseaume et Julien Thorel

- Selon le CEPD, les mesures techniques ne peuvent empêcher efficacement un accès disproportionné des autorités que si même le destinataire des données n'est pas en mesure de les décrypter, de lever le voile sur les pseudonymes ou de les reconstituer. Cela ne peut être envisagé que dans quelques cas, par exemple lorsque les données sont stockées dans le pays tiers uniquement à des fins de sauvegarde.
- Si le destinataire des données a ou doit avoir accès au texte en clair des données à traiter, même les mesures techniques ne protègent pas efficacement contre la surveillance des autorités. Si le destinataire est en possession de la clé de décryptage, il pourrait être obligé de la remettre aux autorités. Les « portes dérobées » dont il est question actuellement dans les logiciels de cryptage contrecarreraient également la protection.
- Si l'exportateur de données ne peut garantir une protection des données équivalente à celle garantie au sein de l'UE par des mesures supplémentaires, il – ou à titre subsidiaire l'autorité de contrôle – doit interdire le transfert des données. Dans le cas des transferts de données vers les États-Unis, cependant, rien ne semble pouvoir empêcher efficacement l'accès aux données par les autorités sur la base des lois de surveillance du pays, dans la mesure où le destinataire a accès aux données.
- Les CCT dans leur version amendée, proposées par la Commission européenne en novembre 2020, ne peuvent offrir un niveau de protection des données équivalent à celui de l'UE que si elles sont complétées de mesures techniques. Afin d'éviter toute ambiguïté supplémentaire, les nouvelles CCT devraient être davantage en adéquation avec les recommandations du CEPD.

Conclusions pour les transferts de données à caractère personnel vers les États-Unis

- Tous les transferts de données vers les États-Unis à des destinataires soumis aux lois de surveillance américaines et qui ont accès au contenu des données en clair sont donc actuellement illégaux. Sont notamment concernés les transferts vers des fournisseurs de services cloud et les transferts au sein de groupes d'entreprises pour la fourniture de services de personnel.
- Les autorités européennes de contrôle de la protection des données devraient fournir des orientations sur les destinataires de données qui sont couverts par les lois de surveillance américaines et sur les transferts qui sont juridiquement problématiques.
- Tant que les États-Unis ne réduiront pas leurs lois de surveillance à la portion congrue et n'offriront pas aux citoyens de l'UE des voies de droit effectives, ni les CCT complétées ni un nouveau bouclier de protection de la vie privée « amendé » ne seront utiles.

Conséquences pour les autres instruments de transfert et les transferts de données vers d'autres pays tiers

- Les observations de la CJUE sur les CCT sont transposables à d'autres instruments de transfert des données tels que les règles d'entreprise contraignantes (ROC). Leur utilisation comporte donc des risques comparables pour les transferts de données vers les États-Unis si les destinataires y sont soumis à des lois de surveillance.
- Il peut aussi exister dans d'autres pays tiers des lois de surveillance qui entrent en conflit avec les CCT. Les exportateurs de données doivent donc également vérifier le niveau de protection pour les transferts de données vers d'autres pays pour lesquels il n'existe pas de décision d'adéquation et compléter les CCT si nécessaire. Les transferts de données vers le Royaume-Uni restent autorisés, du moins pour le moment.
- La Commission européenne doit examiner de manière critique les décisions d'adéquation existantes pour les autres pays tiers afin de déterminer s'ils répondent (encore) aux exigences fixées par la CJUE.

Conclusion

- La solution la plus sûre sur le plan juridique consiste à s'abstenir de transférer des données vers les pays tiers dans les cas décrits ci-dessus, à stocker ces données dans l'UE de telle sorte que les sociétés américaines ou leurs filiales n'aient aucun contrôle sur celles-ci, et à utiliser exclusivement des fournisseurs européens qui répondent à ces exigences.
- Les exigences élevées en matière de protection des données au sein de l'UE divergent avec les pratiques actuelles de transfert. Les exportateurs de données qui ne mettent pas fin aux transferts illégaux de données risquent des amendes élevées. Les projets de recommandations du CEPD ou le projet d'amendement des CCT de la Commission européenne ne promettent une solution à ce dilemme à la fois juridiquement sûre et praticable que pour un nombre limité de cas.
- L'arrêt « Schrems II » offre la possibilité de renforcer les services sécurisés et de haute qualité (par exemple, les clouds) au sein de l'UE. Ce n'est qu'alors que le passage à des prestataires de services implantés dans l'UE constituera une alternative à long terme. La création de Gaia-X, qui sera le premier cloud européen, peut être un pas dans cette direction.