L’Oberlandesgericht de Karlsruhe confirme la licéité d’un contrat cloud passé entre un organe public et un fournisseur de service américain

Michael Montavon, le 5 octobre 2022

La Cour d’appel de Karlsruhe a jugé que le seul fait qu’un fournisseur de services *cloud* soit une filiale d’un groupe américain soumis aux lois américaines ne suffit pas pour conclure à une violation de la protection des données selon le droit européen.

OLG Karlsruhe, Beschluss vom 07.09.2022 – 15 Verg 8/22 – openJur

Les faits

Une société allemande de droit public active dans le milieu hospitalier lance un appel d’offres pour l’acquisition d’une solution informatique dans le cadre d’une procédure de marché public ouverte dans toute l’Union européenne. Les critères de l’appel d’offres contiennent des exigences en matière de protection des données et de sécurité informatique. La solution informatique doit être conforme au RGPD et les centres d’hébergement doivent être situés exclusivement dans l’Espace économique européen.

Le marché est attribué à A. Cette dernière ne fournit pas l’entier de la prestation demandée elle-même, mais recourt aux services *cloud* du sous-traitant B (Amazon Web Services EMEA S.à r.l.) basé au Luxembourg, une filiale de la société C (Amazon Web Services, Inc.) basée aux États-Unis. B assure que ses serveurs sont tous situés en Allemagne ou sur le territoire de l’Union européenne. Le sous-traitant fournit par ailleurs une garantie écrite qu’il ne divulguera pas les données récoltées à un tiers, sauf si cela est nécessaire pour se conformer à la loi ou à un ordre valable et contraignant d’une autorité. Il s’engage dans ce contexte à contester les demandes trop larges ou inappropriées, en particulier celles ne respectant pas le cadre européen relatif à la protection des données.

Un soumissionnaire concurrent attaque cette attribution auprès de la *Vergabekammer* du Bade-Wurtemberg en reprochant à l’offre de A de ne pas être conforme au RGPD en raison du recours au sous-traitant B et de son lien de subordination avec C. Le recours aux services *cloud* sur sol européen, mais dont la société mère est américaine implique, selon lui, un transfert de données illicite vers les États-Unis, et ce indépendamment du lieu d’hébergement des

données. En raison des possibilités d'accès des autorités américaines réservées par le *Cloud Act*, il existe au moins un risque latent que ces dernières puissent accéder aux données externalisées ; cela suffit déjà pour reconnaître l'existence d'un transfert au sens des art. 44 ss RGPD. Or, selon l'arrêt Schrems II de la CJUE, les États-Unis ne disposent pas d'une législation jugée adéquate du point de vue du RGPD. Ce transfert doit par conséquent être qualifié d'illicite.

A se défend en arguant qu'une simple possibilité théorique d'accès depuis l'étranger ne constitue pas un transfert vers ce pays au sens des art. 44 ss RGPD. En outre, A et B ont pris toutes les dispositions complémentaires exigées par la jurisprudence Schrems II lors de l'implication d'un pays tiers dans un traitement de données. Non seulement ils ont fait usage des clauses contractuelles types en matière de protection des données (CCT), mais les données sont aussi chiffrées de sorte qu'elles ne peuvent de toute manière pas être lues par des tiers non autorisés. Finalement, B s'est engagé contractuellement vis-à-vis de A à assurer la prestation demandée conformément aux règlementations de l'Union européenne et de l'Allemagne. Il n'existe ainsi aucun élément concret qui indiquerait un futur non-respect des dispositions du RGPD.

La décision de la *Vergabekammer* du Bade-Wurtemberg (1 VK 23/22)

Par décision du 13 juillet 2022, la *Vergabekammer* du Bade-Wurtemberg donne raison au soumissionnaire concurrent et ordonne l'exclusion de A du marché public. En raison du recours à B dont la société mère est américaine, elle juge que la prestation ne serait pas conforme au RGPD comme l'exigent les critères fixés par l'appel d'offres. Elle estime que le recours aux services cloud de B constitue un transfert illicite de données vers les États-Unis.

Pour arriver à ce résultat, la *Vergabekammer* procède à l'analyse de l'expression « transfert de données » prévue à l'art. 44 RGPD. Elle parvient à la conclusion que celle-ci doit être comprise non pas comme un traitement, mais comme toute divulgation de données. Le recours à B en tant que fournisseur de services *cloud* constitue ainsi un transfert de données au sens des art. 44 ss RGPD.

L'utilisation de l'infrastructure d'hébergement de B comporte un « risque latent » d'accès par des organismes tant publics que privés en dehors de l'UE, notamment aux États-Unis, peu importe que ce dernier ait son siège dans l'UE et que le stockage des données doive se faire exclusivement sur des serveurs en Allemagne ou dans l'UE. Un tel risque latent peut se concrétiser à tout moment. Il suffit à conclure à l'existence d'un transfert de données.

Le RGPD n'autorise pas le transfert de données vers un pays tiers à moins que des garanties spéciales ne soient prévues (sur la question, cf. www.swissprivacy.law/45). Depuis l'arrêt Schrems II, l'usage seul des CCT n'est pas de nature à rendre licite le transfert de données vers les États-Unis et A ne démontre pas concrètement en quoi le chiffrage des données permet de protéger ces dernières d'un accès par des tiers. En concluant un contrat avec B, A perd, partiellement en tout cas, son pouvoir d'influence sur les données dont il est responsable.

Dans le cas présent, le recours aux services de B constitue ainsi un transfert illicite de données vers les États-Unis.

Saluée par certains, cette décision n'a pas fait l'unanimité, y compris auprès de l'Autorité de protection des données du Bade-Wurtemberg. Dans une prise de position du 15 août 2022, cette dernière a qualifié de douteuse l'assimilation faite par la *Vergabekammer* entre le risque d'accès et le transfert de données. Même si elle reconnaît que l'approche fondée sur les risques est généralement trop favorable au responsable du traitement, elle est d'avis que l'approche adoptée par la *Vergabekammer* du Bade-Wurtemberg constitue un revirement de pratique brutal préjudiciable aux responsables du traitement.

Le jugement de l'*Oberlandesgericht* de Karlsruhe (15 Verg 8/22)

Par jugement du 7 septembre 2022, l'*Oberlandesgericht* de Karlsruhe casse la décision du 13 juillet 2022 de la *Vergabekammer* du Bade-Wurtemberget confirme l'attribution du marché public à A.

Elle relève qu'en signant les contrats spécifiques contenant des garanties relatives au respect de la législation européenne en matière de protection des données imposées par A, B fait une promesse de prestation claire et sans équivoque dans laquelle elle garantit que le traitement des données non seulement ne quitterait pas l'Union européenne, mais se ferait uniquement en Allemagne. C'est dans le sens d'une telle promesse contraignante que le pouvoir adjudicateur a également compris les déclarations de A dans les documents d'adjudication. Le pouvoir adjudicateur pouvait légitimement se fier à cette promesse de prestation. Contrairement à ce que pense le concurrent évincé, le seul fait que B soit une filiale d'un groupe américain ne doit pas faire douter le pouvoir adjudicateur de la possibilité de remplir la promesse de prestation. Rien ne permet de dire qu'en raison du lien existant entre B et la société mère américaine, des instructions contraires à la loi et au contrat seraient données à B ou que B, en tant que filiale européenne de C, suivrait, par l'intermédiaire de ses directeurs, des instructions de la société mère américaine qui sont contraires à la loi.

Appréciation

De manière un peu décevante, l'*Oberlandesgericht* de Karlsruhe ne se prononce pas (directement) sur les questions de protection des données sous-jacentes, mais fonde son raisonnement du seul point de vue contractuel. On ne trouve ainsi aucun raisonnement concernant le fait que la *Vergabekammer* du Bade-Wurtemberg assimile le recours à des services cloud européens proposés par un fournisseur américain à un transfert de données illicite vers les États-Unis.

Selon l'opinion que nous défendons, il n'est toutefois pas possible de réprimer un acte illicite qui ne s'est pas encore réalisé au seul motif qu'il existe un risque – peut-il alors être autre chose que « latent » ? – qu'il ne se réalise. Une analogie intéressante peut être faite ici avec la circulation routière. Dès le moment où un véhicule est mis en circulation, on accepte le risque que non seulement le conducteur, mais aussi des tiers (autres usagers, cyclistes, piétons) puissent subir un accident. Ce risque est même très précisément quantifié. Selon les chiffres de l'Office fédéral de statistique, l'année 2021 a connu 20'794 victimes de la route en Suisse dont 200 tuées, 3993 gravement blessées et 16'601 légèrement blessées. Il s'agit donc d'un risque élevé et concret. Pour y remédier, la législation en matière de circulation routière fixe de nombreuses règles de comportement à respecter. Ces règles sont renforcées par des dispositifs de sécurité comme l'installation de ceintures ou d'airbags, la pose de radars ou des contrôles de police. Mais le risque demeure et des accidents surviennent.

Cette même conception se retrouve dans la législation sur le fait des produits défectueux, dans la législation sur la recherche sur l'être humain, dans la législation sur les produits thérapeutiques ou encore dans la législation bancaire et financière. On accepte l'existence d'un risque résiduel, car il n'y a pas vraiment d'alternative. Pourquoi devrait-il en aller différemment dans la législation sur la protection des données ? Dans une interview récente, la Préposée zurichoise à la protection des données a déclaré que l'utilisation de services cloud américains devrait être interdite même si la probabilité d'un accès illicite était de 0,0001 pour cent. Il va sans dire que le droit fondamental à la protection des données est un droit très précieux et qu'il doit être protégé. Mais est-il plus précieux que l'intégrité physique, la vie ou le patrimoine au point de justifier la création d'un nouveau régime de responsabilité sans précédent qui rejette entièrement le risque ?

Proposition de citation : Michael Montavon, L'Oberlandesgericht de Karlsruhe confirme la

licéité d'un contrat cloud passé entre un organe public et un fournisseur de service américain, 5 octobre 2022 *in* www.swissprivacy.law/175