Des données personnelles pseudonymisées transférées à un tiers deviennent-elles anonymes ?

Alexandre Jotterand, le 13 juin 2023

La notion de données personnelles est aussi importante que ses contours sont débattus. Une récente décision du Tribunal de l'Union européenne apporte des éclaircissements importants sur cette notion et son application dans le cadre de transferts de données sous une forme pseudonymisée à un tiers qui ne dispose pas de la clé permettant de déchiffrer les données.

Arrêt du Tribunal de l'Union européenne, Affaire T-557/20 du 26 avril 2023 (CRU / CEPD)

Introduction

Le Tribunal de l'Union européenne (TUE) a rendu un arrêt majeur le 26 avril dernier sur la notion de données personnelles. Cet arrêt, qui n'a pas (encore) fait les gros titres, aura sans aucun doute un impact considérable sur l'application du droit de la protection des données en Europe et dans le monde.

En effet, bien qu'il ne concerne pas le RGPD directement, mais le règlement (UE) 2018/1725 – qui est son pendant pour les traitements de données personnelles effectués par les institutions et organes de l'UE – il apporte pour la première fois depuis l'arrêt de la CJUE « Breyer » des clarifications importantes sur le concept fondamental de données personnelles (respectivement de données à caractère personnel selon la terminologie en droit européen). Nous précisons d'emblée que les dispositions légales sur lesquelles l'arrêt se fonde sont identiques dans le RGPD, et que les principales décisions de justice citées se rapportent au RGPD. Les considérations qui suivent sont donc à notre avis pleinement transposables au RGPD.

Les faits

Le Conseil de résolution unique (CRU) est une autorité européenne dont le but est de contribuer à la stabilité financière en Europe et qui a été chargée du cas de la Banco Popular Español en pleine déroute. Pour les besoins de la procédure, le CRU mandate le cabinet Deloitte afin de procéder à une évaluation des actifs de la banque.

Dans ce cadre, le CRU partage avec Deloitte des commentaires émanant d'actionnaires de la banque. Avant leur transfert à Deloitte, le CRU a supprimé tous les identifiants directs (nom, prénom, etc.) des commentaires et a appliqué un code alphanumérique. Au moyen de ce code, le CRU était le seul à pouvoir relier les commentaires aux individus concernés. Le code alphanumérique est utilisé à des fins d'audit pour permettre de vérifier, et éventuellement de démontrer, *a posteriori* que chaque commentaire avait été traité et dûment pris en compte. Deloitte n'a jamais eu accès à la base de données complète, ni au code permettant de réidentifier les auteurs des divers commentaires.

La déclaration relative au traitement de données à caractère personnel du CRU ne contenait pas d'information sur un potentiel transfert de données personnelles à Deloitte. Partant de ce constat, cinq actionnaires ont introduit une plainte contre le CRU auprès du Contrôleur européen de la protection des données (CEPD [ou EDPS en anglais]), qui est l'autorité européenne chargée de veiller au respect du règlement (UE) 2018/1725 (à ne pas confondre avec le Comité européen de la protection des données, qui porte également en français l'acronyme CEPD [EDPB en anglais], qui lui veille à l'application du RGPD). À la suite des plaintes, le CEPD rend une décision dans laquelle il retient que le CRU a transféré des données personnelles à Deloitte en violation des règles prévues par le règlement (UE) 2018/1725.

Le CRU conteste cette décision auprès du Tribunal de l'Union européenne (TUE). Il estime en substance que les données transmises à Deloitte ne doivent pas être considérées comme des données à caractère personnel, car Deloitte n'était pas en mesure d'identifier les auteurs des commentaires et que Deloitte n'avait donc pas besoin d'être listé comme destinataire des données. De son côté, le CEPD persiste dans sa position, estimant que des données pseudonymisées sont toujours des données à caractère personnel (y compris pour le destinataire qui n'a pas accès au code). Dans son arrêt du 26 avril 2023, le TUE rejette sèchement la position du CEPD et annule sa décision, pour les motifs exposés ci-après.

Un commentaire ne « se rapporte » pas nécessairement à une personne physique

Pour rendre sa décision, le TUE se plonge dans la notion de « données à caractère personnel », qui est définie de manière identique à l'art. 4 par. 1 RGPD et à l'art. 3 par. 1 du règlement (UE) 2018/1725. Il ressort de cette définition qu'une information constitue une donnée à caractère personnel, si quatre conditions cumulatives sont réunies, soit (1) l'existence d'une information, (2) qui « se rapporte » à (3) une personne physique et, enfin, (4) que cette personne soit « identifiée ou identifiable ».

Le TUE rappelle tout d'abord, en référence à l'arrêt de la CJUE « Nowak » (points 34–35), que

la notion d'« information » doit être interprétée de manière large et n'est pas restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toute sorte d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci « concernent » la personne en cause, ce qui sera le cas si son contenu, sa finalité ou son effet est lié à cette personne.

Sur cette base, le TUE juge que le CEPD ne pouvait pas considérer de manière schématique que les commentaires des actionnaires, comme toute opinion personnelle, constituaient systématiquement des informations « se rapportant » à des individus (arrêt commenté, point 73). Selon le TUE, s'il ne saurait être exclu que des points de vue personnels ou des opinions constituent des données à caractère personnel, une telle conclusion doit nécessairement s'appuyer sur l'examen visant à déterminer si, par son contenu, sa finalité ou son effet, un point de vue est lié à une personne déterminée. Le CEPD n'ayant pas fait cette analyse, il ne pouvait retenir que les informations transmises à Deloitte constituaient des informations « se rapportant » à une personne physique.

Des données pseudonymisées sont anonymes pour celui qui ne dispose pas des moyens de ré-identification

C'est toutefois sur l'exigence du caractère « identifiable » de l'information que l'arrêt est le plus intéressant. De manière similaire à l'opinion répandue parmi les autorités chargées de faire appliquer le RGPD, le CEPD avait retenu que des données pseudonymisées sont toujours des données à caractère personnel et qu'il n'existe pas de distinction légale entre ceux qui conservent les données « pseudonymisées » et ceux qui détiennent les informations supplémentaires (le code) permettant une réidentification. Dès lors, le fait que Deloitte n'ait pas été en mesure à lui seul d'attribuer les commentaires aux données reçues lors de la phase d'inscription n'excluait pas que les données qu'il avait reçues étaient pseudonymisées et donc personnelles.

Le TUE s'appuie sur l'arrêt « Breyer » pour contredire la position du CEPD, ainsi que sur le considérant 16 du règlement 2018/1725 (qui est identique au considérant 26 du RPGD). Dans l'arrêt Breyer (rendu avant l'entrée en vigueur du RGPD), la CJUE a jugé en substance qu'afin de déterminer si une information, en l'occurrence une adresse IP, est une donnée à caractère personnel : (1) il convient de prendre en compte les moyens susceptibles d'être raisonnablement mis en œuvre par le détenteur de cette information pour identifier la personne concernée et (2) qu'il n'est en soi pas pertinent que les données supplémentaires permettant l'identification se trouvent en main d'un tiers, pour autant que ces informations puissent léga-

lement être requises et que cela n'implique pas un effort démesuré.

Cette jurisprudence a fait l'objet de nombreux débats juridiques et conduit à des opinions opposées sur la nature plutôt relative ou absolue de la notion de donnée à caractère personnel. L'arrêt commenté ici est à notre connaissance la première décision d'une autorité judiciaire européenne appliquant directement l'arrêt Breyer au RGPD (respectivement au règlement 2018/1725), y compris au considérant 26 du RGPD (qui correspond au considérant 16 du règlement 2018/1725 dans l'arrêt analysé), dont la la teneure est la suivante :

> (26) […] Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. […]

Dans son arrêt, le TUE considère que l'arrêt Breyer, interprété à la lumière du considérant ci-dessus, nécessite d'analyser la possibilité d'une identification du point de vue du destinataire :

> (96) Certes, […] le fait que les informations supplémentaires nécessaires pour identifier les auteurs des commentaires reçus lors de la phase de consultation étaient détenues non pas par Deloitte, mais par le CRU, n'apparaît pas de nature à exclure a priori que les informations transmises à Deloitte constituaient, pour celui-ci, des données à caractère personnel.
>
> (97) Toutefois, il ressort également de l'arrêt du 19 octobre 2016, Breyer (C-582/14, EU:C:2016:779), que, pour déterminer si les informations transmises à Deloitte constituaient des données à caractère personnel, il convient de se placer du point de vue de ce dernier pour déterminer si les informations qui lui ont été transmises se rapportent

> à des « personnes identifiables ».

En définitive, le TUE juge que le CEPD aurait dû rechercher si les auteurs des informations transmises à Deloitte étaient directement identifiables par Deloitte ou si Deloitte disposait de moyens légaux et réalisables en pratique lui permettant d'accéder aux informations supplémentaires nécessaires à la réidentification des auteurs des commentaires. Faute pour le CEPD d'avoir fait cette analyse – ayant considéré que les données pseudonymisées étaient systématiquement des données à caractère personnel, tant pour le CRU que pour Deloitte – le TUE annule la décision du CEPD.

Commentaire

Cet arrêt ouvre de nouvelles perspectives en matière de transmission d'informations pseudonymisées (ou « dé-identifiées ») et apporte une clarification juridique bienvenue sur un concept aussi important que celui de « donnée personnelle ». Il remet en question l'interprétation souvent prônée en tout cas dans l'Union européenne selon laquelle les données pseudonymisées restent systématiquement des données personnelles, même lorsqu'elles sont transmises à des tiers qui ne disposent ni des informations supplémentaires nécessaires pour réidentifier les personnes, ni d'un moyen licite de les obtenir.

Selon l'arrêt du TUE, le caractère identifiable de l'information doit être analysé du point de vue de la personne qui détient l'information. En conséquence, la même information peut être une donnée personnelle pour un acteur, et une donnée anonyme pour un autre, en fonction des moyens raisonnablement disponibles à chacun d'eux. Ainsi, le TUE adopte (à raison) une approche fondée sur le risque d'identification dans chaque scénario individuel, plutôt qu'une approche absolue.

Cet arrêt rapproche la conception européenne de la notion de donnée personnelle de celle prévalant en Suisse, que l'auteur de cet article a analysée dans une récente publication dans la Jusletter (Alexandre Jotterand, Personal Data or Anonymous Data : where to draw the lines (and why)?, in : Jusletter 15 August 2022 (disponible à cette adresse) ; laquelle a fait l'objet d'une recension sur www.swissprivacy.law/202). En résumé, l'analyse de la possibilité d'identification (directe ou indirecte) doit dans le cadre de la LPD (et de la nLPD) également partir du point de vue du détenteur de l'information, et prendre en compte l'environnement dans lequel les données sont partagées. Tout comme dans l'arrêt analysé ici, il n'est pas pertinent en cas de transfert que les données soient qualifiées de personnelles pour celui qui les transmet : c'est le point de vue du destinataire qui doit être analysé. Si le destinataire

n'est pas en mesure d'identifier les personnes concernées, que se soit directement ou à l'aide d'informations supplémentaires raisonnablement accessibles auprès d'un tiers, il faut alors retenir qu'aucune donnée personnelle ne lui est communiquée.

Cette situation à l'avantage d'éviter l'application par exemple des règles sur le transfert international de données personnelles ou concernant la communication de données sensibles à des tiers (puisque ce qui est reçu par le destinataire n'est pas des données personnelles).

Ces avantages sont toutefois tempérés de plusieurs manières :

- La situation présente certains risques pour celui qui transmet les données : en effet, alors que les données restent en principe pour lui des données personnelles (puisqu'il détient le code), le destinataire des informations ne sera, lui, pas soumis à la LPD (ou au RGPD), puisque les données ne seront pas pour lui des données personnelles. Cette situation peut poser des problèmes à celui qui transfère des données, qui s'est potentiellement engagé envers les personnes concernées à traiter les données d'une certaine manière. Au demeurant, en cas de violation de la sécurité des données chez le destinataire, celui-ci ne sera légalement pas tenu de notifier le responsable du traitement (l'art. 24 nLPD ne lui sera en principe pas opposable), alors que le responsable du traitement sera quant à lui tenu à des obligations d'annonce.
- L'analyse juridique dépend d'une situation factuelle spécifique (le *data environment*), basée sur les moyens raisonnablement à disposition du destinataire. Si la situation factuelle change, par exemple parce que le destinataire transmet à son tour les données (qui sont anonymes pour lui) à des tiers, ou les publie sur internet, l'analyse juridique change également et des données qui ont été anonymes pendant un moment peuvent soudainement redevenir personnelles.
- Enfin, l'analyse juridique complète dépend du rôle de chaque acteur : elle sera en partie différente en cas de transfert entre un responsable du traitement et son sous-traitant, ou entre des responsables conjoints du traitement.

Celui qui transmet des données pseudonymisées à un tiers sera donc bien inspiré de s'assurer contractuellement que ce tiers se soumettra à des exigences appropriées même si les données ne sont pas personnelles pour lui.

Enfin, il est important de noter que la décision du TUE ne fixe pas de seuil précis pour déterminer si les personnes concernées sont (ré-)identifiables et précise que cela doit être évalué au cas par cas. À ce titre, il aurait été intéressant que le Tribunal se réfère à la récente norme ISO/IEC 27559:2022, dont l'ambition est de servir de cadre pour la désidentification de

données pour la protection de la vie privée. Nous précisons enfin que l'arrêt du TUE peut encore être contesté devant la CJUE. Nous ne manquerons pas d'analyser cette décision subséquente si cela devait être le cas.

Proposition de citation : Alexandre JOTTERAND, Des données personnelles pseudonymisées transférées à un tiers deviennent-elles anonymes ?, 13 juin 2023 *in* www.swissprivacy.law/232

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.