PROTECTION DES DONNÉES

L'impact de l'annulation du « Privacy Shield » pour les collectivités

La Cour de Justice européenne a fait tomber, le 16 juillet 2020, le bouclier de protection des données entre l'UE et les Etats-Unis. Un séisme dans le droit informatique mais aussi dans les pratiques des collectivités. Celles-ci n'ont pourtant pas modifié leurs habitudes de travail, du fait de trop rares alternatives, des réticences et du manque d'accompagnement de l'autorité de contrôle.

1 « PRIVACY SHIELD » : DE QUOI PARLE-T-ON ?

Depuis le 1er août 2016, le régime juridique du « Privacy Shield » permettait de transférer des données personnelles de citoyens membres de l'Union européenne vers les Etats-Unis, à condition que les entreprises destinataires des données se soient préalablement inscrites sur le registre tenu par l'administration américaine. Cette inscription sur le registre garantissait que lesdites entreprises respectaient les obligations et les garanties de fond prévues par le « Privacy Shield ».

Avec ce régime juridique, les entreprises et administrations européennes devaient s'assurer que la société américaine disposait d'une certification active (les certifications devaient être renouvelées tous les ans) et que celle-ci couvrait bien le type de données transférées.

Toutes les sociétés américaines qui avaient accompli avec succès le processus d'auto-certification étaient répertoriées sur la liste du bouclier de protection des données.

Auto-certification ou clauses contractuelles

Les transferts de données vers les Etats-Unis étaient donc libres lorsqu'ils étaient effectués vers des entreprises qui avaient auto-certifié leur adhésion aux principes de protection des données. De fait, l'essentiel des transferts vers les principales entreprises de nouvelles technologies reposait sur le « Privacy Shield ». Pour les autres, ces transferts devaient passer par d'autres mécanismes plus contraignants, telles l'adoption de clauses contractuelles types entérinées par la Commission européenne, de clauses contractuelles ad hoc ou des règles d'entreprises contraignantes.

Un bouclier qui implose

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt majeur invalidant ce régime de transferts des données entre l'Union européenne et les Etats-Unis, précipitant les responsables de traitement européens de données dans des difficultés juridiques et opérationnelles quasiment insurmontables.

2 L'ARRÊT « DATA PROTECTION COMMISSIONER CONTRE FACEBOOK »

Dans son arrêt du 16 juillet 2020 « Data Protection Commissioner contre Facebook Ireland Ltd et Schrems », la CJUE s'est concentrée sur deux grands axes du transfert de données entre l'Europe et les Etats-Unis tels que définis par la juridiction irlandaise.

S'agissant du « Privacy Shield »

D'une part, la CJUE a examiné la validité de la décision relative au bouclier de protection de la vie privée (décision 2016/1250 sur le caractère adéquat de la protection assurée par le bouclier de protection de la vie privée entre l'UE et les États-Unis). Comme l'indique la Cnil dans le travail d'explication qu'elle a faite de cette décision, la CJUE a estimé que les exigences du droit américain – et en particulier certains programmes permettant l'accès des autorités publiques américaines aux données personnelles transférées de l'UE vers les Etats-Unis à des fins de sécurité nationale –, entraînent des limitations de la protection des données personnelles qui ne sont pas circonscrites de manière à satisfaire à des exigences essentiellement équivalentes à celles requises par le droit de l'UE.

Lorsque la Cnil répond aux questions posées par l'annulation du « Privacy Shield », elle rappelle que la CJUE considère que cette législation n'accorde pas aux personnes concernées des droits de recours devant les juridictions contre les autorités américaines. La CJUE souligne ainsi que certains programmes de surveillance permettant l'accès des autorités publiques américaines aux données personnelles transférées de l'UE vers les Etats-Unis à des fins de sécurité nationale ne prévoient aucune limitation du pouvoir conféré aux autorités américaines,

ni l'existence de garanties pour les personnes potentiellement ciblées non américaines. Aussi, dans la mesure où les atteintes portées aux droits des Européens sont particulièrement graves, la CJUE a choisi de rendre la décision d'adéquation du « Privacy Shield » caduque.

S'agissant des clauses contractuelles types

D'autre part, la CJUE a examiné la validité de la décision 2010/87/CE de la Commission européenne relative aux clauses contractuelles types. A l'inverse de qui a été décidé concernant le « Privacy Shield », la CJUE a validé la décision de la Commission européenne relative aux clauses contractuelles types.

Dans sa lecture de la décision, la Cnil a retenu que la validité des clauses ne peut pas être remise en cause uniquement par le fait que leur nature contractuelle ne lie pas les autorités du pays tiers vers lequel les données peuvent être transférées.

Elle constate également que ces clauses types prévoient des mécanismes effectifs permettant en pratique de suspendre ou d'interdire les transferts lorsque l'entité destinataire ne respecte pas ou est dans l'incapacité de respecter ces clauses, si bien que leur validité n'est pas remise en cause. En revanche, en fonction de l'état du droit de l'Etat destinataire, il appartient à l'exportateur de données d'adopter des mesures complémentaires afin d'assurer le respect d'un niveau de protection adéquat.

3 CONSÉQUENCES POUR LES COLLECTIVITÉS

Cet arrêt de la CJUE emporte diverses conséquences pratiques pour les collectivités utilisant des logiciels américains. En effet, les collectivités territoriales, avec le premier confinement, ont pu être tentées d'acquérir des licences de logiciels américains pour stocker et échanger des documents, mettre en place des outils statistiques ou encore des logiciels de visioconférence contenant nécessairement des données à caractère personnel. L'impact de la décision de la Cour de justice de l'Union européenne est primordial, puisque l'on considère maintenant que les sociétés américaines transféreront à leurs autorités nationales, en raison de la législation américaine sur la sécurité nationale, des données à caractère personnel de citoyens européens alors même que ces atteintes ne sont pas circonscrites de manière à satisfaire à des exigences essentiellement équivalentes à celles requises par le droit de l'UE.

A ce jour, aucun moyen technique ou organisationnel ne permet de transférer des données à caractère personnel en toute sécurité juridique vers les Etats-Unis.

Des outils devenus inutilisables

Aussi, en théorie, il n'est plus possible pour les collectivités territoriales d'utiliser en l'état ces outils. En effet, la première et la principale conséquence de cet arrêt est que la seule adhésion au « Privacy Shield » des entités américaines destinataires ne suffit plus à rendre légal le transfert de données depuis l'Union européenne.

Rappelons que les articles 46 et suivants du RGPD exposent les différents choix pouvant s'offrir à vous dans le cadre de l'envoi de données à caractère personnel dans un pays non adéquat. L'article 46 présente sept solutions antérieures à l'envoi :

– des clauses contractuelles types (« CCT ») de la Commission européenne ;
– des clauses contractuelles spécifiques écrites ad hoc ;
– des règles internes et contraignantes d'entreprises lorsqu'elles ont une dimension internationale (souvent désignées « BCR » pour Binding Corporate Rules ; concernant des transferts internationaux intragroupes) ;
– des clauses contractuelles types adoptées par une autorité de contrôle et approuvées par la Commission européenne ;
– un code de conduite approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) ;
– un mécanisme de certification approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) ;
– un arrangement administratif ou un texte juridiquement contraignant et exécutoire pris pour permettre la coopération entre autorités publiques.

Or, dans la situation des collectivités, seules les solutions relatives aux clauses contractuelles de la Commission sont réellement envisageables.

Pour le reste, il n'y a pas à ce jour de clauses contractuelles types adoptées par la Cnil et validées par la Commission européenne, ni de code de conduite, de mécanisme de certification ou encore d'arrangement administratif en matière de données. Et les règles internes d'entreprises (internationales) ne sont pas transposables aux personnes publiques locales. ●●●

RÉFÉRENCES

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Décision de la Commission européenne du 12 juillet 2016 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE/Etats-Unis
- « Invalidation du Privacy Shield : les premières questions-réponses du Comité européen de la protection des données », article de la Cnil du 31 juillet 2020

●●● Cependant, la problématique résulte ici du fait que le recours aux clauses contractuelles types comme seul outil d'encadrement des transferts de données vers les Etats-Unis est devenu indirectement inopérant. La CJUE a constaté que plusieurs textes de loi américains (PISA et Executive Order notamment) n'assuraient pas un niveau de protection suffisant pour permettre un transfert de données personnelles d'Européens vers les Etats-Unis. En effet, on voit difficilement comment des clauses contractuelles signées avec les entreprises américaines pourraient refuser de communiquer des données personnelles de citoyens de l'Union européenne

Quelles mesures complémentaires prendre ?

Aussi, la CJUE a évoqué le besoin de prendre des mesures complémentaires afin d'assurer un niveau de protection adéquat aux données transférées, sans jamais préciser lesquelles. En effet, elle ne mentionne jamais quelles mesures seraient de nature à rendre ce transfert licite. Il appartient maintenant aux autorités de contrôle européennes d'apporter, ensemble, des éléments de réponse. Aussi, il existe une grande incertitude juridique. Il semble que la décision de la CJUE n'ait pas une dimension très pratique, en ce sens que les clauses contractuelles types sont toujours valides mais seulement si des mesures complémentaires sont prises alors qu'on n'en connaît pas la nature.

Par ailleurs, on voit difficilement quelles mesures complémentaires pourraient être prises par des collectivités européennes avec leurs homologues américaines qui seraient suffisamment contraignantes pour faire barrage aux lois sécuritaires américaines.

Dans cette situation, on peut regretter que la Cnil n'ait pas joué son rôle d'accompagnateur des administrations et des entreprises en ne proposant pas des solutions concrètes auprès des structures touchées par l'invalidation de la décision d'adéquation du « Privacy Shield » mais se soit contentée d'expliciter le contenu de la décision sur son site internet.

4 RESPONSABILITÉ DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

En tout état de cause, il appartient à l'ensemble des délégués à la protection des données (DPO) d'être lucides quant aux bouleversements induits par la décision de la CJUE. On peut légitimement penser qu'il n'existe aucun moyen technique ou organisationnel permettant de transférer des données à caractère personnel en toute sécurité juridique vers les Etats-Unis à ce jour en dehors d'un procédé de chiffrement.

Tous les autres outils pouvant être mis en œuvre ne feront jamais barrage aux lois américaines sur la sécurité nationale. C'est aussi en cela que la Cnil et ses homologues européennes ont probablement du mal à expliquer quels seraient les moyens complémentaires en mesure de rendre un tel transfert licite. A l'instar de ses homologues européennes, la Cnil se trouve ainsi dans l'incapacité d'accompagner les responsables de traitements et n'offre aucune solution, alors même qu'il n'existe parfois aucun outil alternatif satisfaisant susceptible d'éviter un tel transfert de données.

De ce fait, les collectivités n'ont d'autre possibilité que d'attendre la publication d'une nouvelle décision d'adéquation dans les prochaines semaines entre l'Union européenne et les Etats-Unis.

Le rôle accru du DPO

Durant ce délai, le rôle des DPO des collectivités va s'avérer primordial. Ils vont devoir communiquer en interne sur la nouvelle décision européenne et ses conséquences et définir des recommandations internes qui auront pour objectif d'inviter les différents acteurs manipulant des données à caractère personnel à anonymiser tout ce qui peut l'être dans l'usage des outils américains, de minimiser autant que possible l'utilisation de ces logiciels ou de recueillir un consentement exprès de chaque personne concernée.

Privilégier les prestataires européens

Plus que jamais, il convient de matérialiser des recommandations inspirées du guide de sécurité de la Cnil de juin 2018, dans une charte des bons usages des outils informatiques intégrant les conséquences de la décision de la CJUE.

Au-delà, un modèle d'avenant devrait être rédigé avec différentes clauses contractuelles types et adressé aux entités destinataires américaines pour témoigner de la proactivité de la structure.

Enfin, il serait judicieux de se tourner, chaque fois que possible (et dans le respect des règles de la commande publique) vers des prestataires européens proposant le même type de service que les outils américains. L'ensemble de ces éléments permettront, en cas de contrôle, de montrer la bonne volonté et la proactivité de la structure sur les conséquences de cette décision.

La décision de la CJUE bouleverse l'ordre établi et impacte considérablement les transferts de données à caractère personnel vers les Etats-Unis. Il ne semble pas qu'il y ait aujourd'hui un quelconque outil permettant d'apporter des moyens complémentaires suffisants pour assurer ces transferts en toute légalité.

Par David Conerardy et Aloïs Ramel,
avocats à la cour, SCP Seban et associés