ENCADREMENT DES FLUX INTERNATIONAUX DE DONNEES PERSONNELLES

Livre Blanc

Décembre 2021

DS AVOCATS

SOMMAIRE

****

Depuis la décision « *Schrems II* » de la Cour de Justice de l'Union Européenne du 16 juillet 2020, l'encadrement de nombreux flux transfrontaliers de données personnelles est compromis. En effet, non seulement cette décision a acté de l'invalidation du *Privacy Shield* (programme américain de conformité à la législation européenne), mais elle a fragilisé les modes alternatifs d'encadrement des transferts que sont les Clauses Contractuelles Types de la Commission européenne (CCT, du moins dans leur version de 2010) ou les Règles Contraignantes d'Entreprise adoptées par certains groupes internationaux (BCR) pour appliquer la protection des données personnelles des européens quels que soient les localisations et entités chargées en leur sein de traiter ces données.

Désormais donc, ces « garanties » ne sont plus absolues si la législation du pays d'accueil prévoit des cas de divulgation aux autorités étrangères sans protection suffisante pour les personnes concernées. Ces débats, qui durent maintenant depuis plusieurs années, sont liés aux révélations d'Edouard Snowden sur les programmes américains de surveillance qui permettent de gigantesques collectes de données à l'échelle mondiale, à l'insu des personnes et sans véritable contrôle démocratique.

Mais les programmes américains ne sont pas seuls en cause. De nombreux pays déploient des mesures de surveillance de leurs populations et des populations étrangères, parfois très larges et intrusives, mais justifiées par des impératifs de sécurité nationale, de lutte contre la criminalité (voire parfois de manière moins avouable, par des calculs politiques ou des affrontements économiques - et c'est un truisme de rappeler la concurrence qui oppose acteurs commerciaux américains et européens).

Ces mesures de surveillance globale posent de nombreux problèmes au regard des libertés publiques, et tout particulièrement au regard de la protection des données personnelles. Or le Règlement Général sur la Protection des Données (RGPD), qui est le cœur du droit européen en la matière, prévoit qu'une donnée personnelle ne peut être collectée que de manière transparente, en préservant les droits de la personne concernée, et pour des finalités licites préétablies.

Concrètement, dès qu'une entreprise française confie ses données personnelles à un prestataire soumis à une législation étrangère, la législation étrangère naturellement applicable à ce dernier est susceptible de contredire les exigences du RGPD et, dans les faits, d'amoindrir ou nier la protection des données personnelles des européens.

Or, un très grand nombre d'entreprises françaises et européennes procèdent à de tels transferts, ou s'appuient sur des sous-traitants qui procèdent à ces transferts, au premier rang desquels les piliers de l'économie numérique que sont Microsoft, Amazon, Google, Oracle ou Facebook, pour ne citer que les plus évidents. Ces entreprises recherchent donc aujourd'hui le moyen de sécuriser ces flux en considération des préconisations émises par le Contrôleur Européen à la Protection des Données (CEPD, ancien Groupe Art. 29).

1. LA REMISE EN CAUSE DES GARANTIES ENCADRANT LES FLUX TRANSFRONTALIERS

1.1 La décision « Schrems II » de la CJUE du 16 juillet 2020

Dans l'affaire « *Schrems II* » du 16 juillet 2020, la CJUE a annulé la décision de la Commission européenne n°2016/1250 du 13 avril 2016 qui avait avalisé le « *bouclier de protection des données UE-Etats-Unis* » (*Privacy shield*). Ce Privacy Shield, qui permettait depuis 2016 de poursuivre le transfert de données personnelles d'européens vers des prestataires américains, avait été mis en place suite à l'invalidation du précédent programme américain (*Safe Harbor*) suite à une première affaire « *Schrems I* ».

En 2016, il s'est avéré que le *Privacy Shield* encourait une bonne partie des critiques précédemment adressées au *Safe Harbor* : dans les deux cas, la CJUE a estimé que le programme américain était au final une pétition de principe, et non une garantie effective assurant la protection des données des européens traitées aux USA.

Or depuis son entrée en vigueur effective en 2018, les dispositions du RGPD interdisent toute demande d'accès d'une autorité d'un pays tiers, adressée à des entreprises dont les traitements sont soumis au RGPD, en dehors d'un accord international spécifique (ou d'une dérogation relative à l'intérêt vital de la personne concernée).

La première conséquence, immédiate, est que tous les flux transfrontaliers encadrés uniquement par le *Privacy Shield*, sont devenus *ipso facto* illicites. Aucun délai de grâce n'étant accordé par la Cour, il était urgent pour l'ensemble des entreprises européennes qui recourent à des prestataires européens, de vérifier leurs contrats et d'adopter d'autres garanties telles qu'autorisées par les articles 44 et suivants du RGPD.

Cette décision repose sur le fait que le *Privacy Shield* n'apportait pas les garanties nécessaires de compatibilité avec le RGPD, face aux programmes de surveillance américains qui permettent aux autorités locales d'accéder aux données hébergées, détenues ou traitées par des prestataires américains - que cela soit via des serveurs situés sur le territoire américain, ou partout ailleurs dans le monde si ces serveurs sont opérés par les prestataires américains.

Dans sa décision, la CJUE maintenait par ailleurs le principe d'une compatibilité des transferts avec le RGPD s'ils sont réalisés sur la base des clauses contractuelles types (CCT)… mais n'accordait pas non plus un blanc-seing à cet égard.

La décision de la CJUE indique qu'il incombe désormais aux responsables de traitement qui continuent de déclencher l'envoi de données vers des prestataires américains en vertu de CCT ou de BCR, de déployer des « *mesures additionnelles pour assurer le niveau de protection des données requis* ». Autrement dit, là où le droit local compromet la protection des données personnelles, c'est aux entreprises qui procèdent au transfert de déployer des mesures pour contrer la faille.

Ce point évacue définitivement la fausse solution consistant pour les prestataires étrangers à acheter des datacenters sur le territoire européen pour se prétendre conformes au RGPD : c'est la nationalité de ces prestataires qui constitue le cheval de Troie via lequel les autorités étrangères peuvent accéder aux données, quand bien même elles ne quittent jamais le territoire de l'EEE.

Il ne s'agit finalement ici que d'une nouvelle illustration des conflits de loi qui se manifestent lorsqu'une entreprise est à la fois soumise à une législation étrangère en vertu de sa nationalité, et au RGPD en vertu des données personnelles qu'elle traite, pour son compte ou pour le compte d'entreprises européennes. Mais cette question classique a pris une acuité nouvelle, et particulièrement acérée, suite à la décision de la CJUE, au point de placer les entreprises européennes devant un dilemme quasiment insoluble.

1.2 Les premières préconisations du Comité Européen de Protection des Données (CEPD) du 23 juillet 2020.

Au lendemain de la décision de la CJUE, le CEPD a publié un ensemble de questions-réponses, où il confirme que l'on ne peut plus se contenter de la simple signature des CCT. Puisqu'il est confirmé au plus haut niveau juridictionnel européen que les réglementations US posent problème, on doit s'assurer que la protection des CCT (et notamment la restriction d'accès aux autorités US à défaut de garantie de recours suffisante) est bien effective.

Plus précisément, le CEPD indique que les responsables de traitement doivent mener une analyse juridique pour vérifier la compatibilité du droit local avec le RGPD, et si cette étude révèle une incompatibilité, mettre en place des « *mesures additionnelles* » pour y remédier[1].

Or, s'agissant des USA du moins, une telle étude pourrait difficilement conclure différemment de la CJUE elle-même : on sait désormais que la réglementation US en cause (Section 702 FISA and EO 12333 visés dans la décision *Schrems II*) incluant les programmes de surveillance US, mais aussi le fameux CLOUD Act voté en mars 2018, permettent la collecte des données par les autorités US sans le consentement des personnes, et sans leur fournir un recours procédural suffisamment indépendant et impartial.

Le CLOUD Act en particulier, permet aux autorités américaines d'accéder aux données stockées sur les datacenters de toute entreprise de droit américain, même s'il s'agit d'une filiale hors des USA, et même si le datacenter est situé ailleurs dans le monde – y compris sur le territoire de l'UE. Il ne faut pas douter que cette législation spécifique a été pensée en réaction au RGPD et s'inscrit dans la compétition économique acharnée entre prestataires américains et européens.

Cette faculté d'accès aux données, par les autorités étrangères, est particulièrement critique dans le cas des communications électroniques et connexions internet, mais cela concerne plus largement tout traitement de données effectué par des entités américaines. Tous les grands cloud providers US sont concernés, mais aussi tous prestataires US susceptibles d'héberger, traiter ou même seulement consulter des données personnelles d'européens couvertes par le RGPD, où que ce soit dans le monde.

Les exceptions de l'article 49 du RGPD, évoquées dans les recommandations du CEPD, ne peuvent concerner que des transferts *occasionnels*, ou fondés sur un intérêt public « *important* ». En pratique, ces exceptions ont du mal à trouver application dans tous les cas où les entreprises s'appuient sur des éditeurs cloud pour l'exécution de leurs tâches quotidiennes (hébergeurs, SIRH, outils commerciaux et marketing, messagerie électronique, etc.) ou pour traiter de grandes masses de données.

Si l'analyse juridique susmentionnée conclut à une incompatibilité persistante entre la législation étrangère et le RGPD, les entreprises européennes doivent alors renoncer aux transferts, et donc renoncer aux services des prestataires américains – perspective qui place la plupart des DSI et services marketing français dans une situation diabolique.

[1] « *Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee* ».

Le CEPD a produit en urgence des recommandations décrivant l'analyse juridique préalable et les « *mesures additionnelles* » à déployer au cas par cas, publiées le 10 novembre 2020 et accompagnées d'un second texte relatif aux « *Garanties Essentielles Européennes* » du même jour (cf. *infra*). Malheureusement, ces recommandations sont loin de régler les difficultés qui ont surgi depuis 2020.

Ces premières limitations à ce que peuvent faire les entreprises ayant été rappelées, dès le début du mois de mars, compte tenu du caractère sensible des données de santé *même en période de crise.*

2. LES RECOMMANDATIONS CEPD DU 10/11/2020 SUR LES MESURES ADDITIONNELLES

2.1 Synthèse

Dans une première recommandation n°01/2020, le CEPD répète l'un des enseignements de la décision de la CJUE : les responsables de traitement doivent s'assurer que la législation étrangère ne contredit pas le RGPD[2]. Le CEPD lui trouve même un fondement direct dans l'article 5.2 du RGPD : « *Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).* »

En conséquence, le CEPD recommande de suivre les quatre étapes suivantes dans la mise en conformité des flux transfrontaliers concernés :

i. « **Connaître ses flux** » : cartographier les transferts effectués vers des pays tiers (pas seulement les USA), ce qui est de toute façon une obligation établie de longue date, et un préalable indispensable à la conformité RGPD de l'entreprise ;

ii. « **Vérifier les garanties encadrant les transferts** » : En l'absence d'une décision d'adéquation de la Commission européenne, on doit nécessairement recourir à l'un des outils prévus au chapitre V du RGPD ;

iii. **« Vérifier si la législation du pays destinataire peut amoindrir l'effectivité du RGPD** » : Le CEPD confirme ici que c'est à l'entreprise européenne, « *exportatrice des données* », d'effectuer l'étude juridique du droit du pays d'accueil, « *en collaboration avec l'importateur* » (c'est-à-dire par exemple le prestataire américain). Mais il s'agit là de toute loi du pays d'importation, c'est-à-dire tout texte relatif notamment au renseignement militaire, à la sécurité nationale, etc., soit un corpus réglementaire particulièrement dense et complexe ! En France, l'AFCDP a immédiatement indiqué qu'il était disproportionné et irréaliste de mettre à la charge des entreprises une analyse détaillée des législations étrangères, qu'en pratique seuls des juristes du pays d'importation sauront mener ;

[2] « *controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools* ».

iv. « **Identifier et adopter des mesures additionnelles** » nécessaires pour assurer le niveau de protection des données. Le CEPD donne en fin de sa recommandation des exemples de mesures additionnelles, à charge pour le Responsable de traitement de vérifier leur effectivité. Et de conclure que si aucune mesure additionnelle ne suffit, le traitement est à interrompre, tout simplement.

A ces quatre étapes s'ajoute la réévaluation périodique de l'efficacité de ces mesures (ce qui implique par conséquent de mettre en œuvre une veille juridique des évolutions de la législation des pays destinataires en plus de l'analyse initiale).

2.2 L'accountability appliquée aux flux transfrontaliers

Le CEPD rappelle que le RGPD est une réglementation dynamique : les européens ne peuvent se contenter passivement de simples déclarations de conformité émanant des prestataires étrangers. Il leur appartient de définir et déployer les mesures contractuelles, techniques et organisationnelles qui assureront *l'effectivité* de la protection, et d'en faire la preuve auprès des personnes concernées et des autorités de contrôle comme la CNIL.

Dans la mesure où le transfert d'une donnée personnelle est un traitement, le devoir d'*accountability* s'applique à la conformité réglementaire de ce transfert et des traitements réalisés à l'étranger *ou par une entité étrangère*. Dans ce contexte, les exportateurs de données (responsables de traitement ou sous-traitants) doivent s'assurer que la protection qu'ils mettent en place évoluera en fonction du contexte légal, et les importateurs de données (sous-traitants ou sous-traitants ultérieurs dans les pays étrangers ou soumis à législation étrangère) doivent apporter leur concours dans ces vérifications et mises à niveau périodiques.

A cet égard, le CEPD indique d'ailleurs que l'importateur de données doit prévenir l'exportateur de tout changement de la législation du pays d'accueil susceptible d'avoir un impact sur la protection des données. Depuis quelques mois, les cocontractants se livrent donc à des discussions complexes pour déterminer qui, du responsable de traitement européen ou du destinataire à l'étranger (i.e. une filiale, un sous-traitant ou un sous-traitant ultérieur), doit assurer cette veille et adapter ses mesures de protection.

Malheureusement, en pratique les entreprises européennes disposent rarement de la faculté de mettre en œuvre une telle analyse, et a fortiori une veille de l'évolution juridique des pays tiers, puisque cela implique de disposer de juristes formés au droit étranger en cause. Quant aux prestataires, ils ne disposent pas non plus nécessairement des compétences juridiques requises, n'ont pas pour mission de fournir un conseil légal, ou estiment qu'une telle veille engendrerait des coûts supplémentaires à refacturer au client.

Le flou règne donc à ce jour, dans les faits, pour définir qui est le mieux à même de vérifier la conformité de la législation du pays d'accueil avec les exigences du RGPD. Et la question ne concerne pas que les USA, mais tout pays dont la législation n'est pas considérée comme « adéquate » par les CNIL européennes, dont par exemple l'Inde ou les pays du Maghreb qui accueillent beaucoup de filiales sous-traitantes.

2.3 Cartographier les transferts de données

Le responsable de traitement (ou le sous-traitant qui préside à l'exportation des données) doit d'abord identifier les traitements en cause. Le CEPD reconnaît que la tâche peut être difficile[3], mais l'exigence n'est pas amoindrie pour autant.

Cette cartographie des flux est en principe traduite dans le registre des traitements. Attention, le RGPD rappelle que la cartographie va jusqu'à contrôler les « *transferts ultérieurs* », c'est-à-dire des flux qui sont réalisés non pas par le sous-traitant, mais par un sous-traitant ultérieur… Cela a notamment un impact dès qu'un prestataire de la chaine de sous-traitance utilise des services cloud pour travailler : on peut en effet trouver des outils professionnels fournis par les cloud providers américains ou étrangers à chaque étape de la chaine de sous-traitance. Et rares sont les registres de traitements qui atteignent ce degré de granularité dans l'information.

Le CEPD rappelle qu'au passage, le principe de *minimisation* doit être respecté (données uniquement pertinentes et proportionnées aux finalités poursuivies, accès limités au strict nécessaire, durées de conservation définies et respectées). Donc seules les données indispensables pour l'activité sous-traitées peuvent être transférées, pour la seule durée de l'activité transférée.

Le CEPD rappelle également qu'un transfert n'est pas seulement l'envoi technique des données vers le territoire étranger ; il peut aussi s'agir d'une collecte effectuée en ligne, l'observation des données (et leur analyse) depuis l'étranger, ou d'une simple consultation à titre principal ou incident pour l'activité sous-traitée.

L'exigence de cartographie n'est toutefois pas neuve : elle existe depuis l'adoption du RGPD en 2016. Les CNIL considèrent donc qu'en 2021, les entreprises ont procédé à ces cartographies, et connaissent désormais les pays destinataires vers lesquels leurs données sont susceptibles d'être envoyées. En d'autres termes, il n'est plus possible de « découvrir » aujourd'hui que des données personnelles sont envoyées par un sous-traitant ou une filiale vers un pays ou un destinataire qui ne présente pas toutes les garanties nécessaires au regard du RGPD.

2.4 Identifier les garanties encadrant les transferts

Si le pays d'accueil a fait l'objet d'une décision d'adéquation (prononcée par les autorités pour confirmer qu'un pays d'accueil dispose d'une législation équivalente au RGPD), et dans la mesure où cette décision n'est pas révoquée, il n'y a rien d'autre à faire : la loi du territoire d'accueil est aussi protectrice que le RGPD lui-même[4].

Mais même une décision d'adéquation n'est pas une garantie absolue : bien que la législation des USA ait été reconnue comme « adéquate » par les décisions 2000/520 puis 2016/1250 de

[3] « *Recording and mapping all transfers can be a complex exercise for entities engaging into multiple, diverse and regular transfers with third countries and using a series of processors and sub-processors* »

[4] A ce jour, cela concerne Andorre, l'Argentine, le Canada, les Iles Faeroe, Guernesey, Israël, l'Ile de Man, le Japon, Jersey, la Nouvelle Zélande, la Suisse et l'Uruguay. Des discussions sont en cours pour la Corée du Sud. Donc tous les autres pays d'exportation impliquent de mettre en place l'une des garanties prévues aux articles 46 et suivants du RGPD.

la Commission européenne, cela n'a pas empêché les dossiers *Schrems I et II* de conduire à l'invalidation successive du *Safe Harbor* puis du *Privacy Shield*…

En l'absence d'une décision d'adéquation valide[5], on doit déployer l'une des autres garanties prévues par le RGPD : clauses contractuelles types (CCT), règles contraignantes d'entreprise (BCR), codes de conduite, mécanismes de certification, etc. Or, comme l'enseigne la situation actuelle, ces garanties sont considérées comme nécessaires, mais plus forcément suffisantes.

2.5 Analyser si les garanties mises en place sont effectives

La garantie choisie ne doit pas être qu'une affirmation formelle ou un simple engagement contractuel : elle doit être *effective*, et ne pas être contredite dans les faits par la législation locale. Le CEPD confirme donc qu'on doit bien procéder à une analyse de la législation locale[6].

L'assistance due par l'importateur (sous-traitant ou responsable de traitement conjoint ou autonome) est mise en exergue[7] – mais elle fait l'objet d'âpres discussions lors des négociations contractuelles, beaucoup de prestataires tentant de la monnayer.

Cela permet de répondre à une première question s'agissant de l'analyser à mener sur la législation locale : l'importateur des données est le mieux placé pour rendre compte de cette législation et indiquer si elle présente des contradictions avec le RGPD. Les entreprises françaises peuvent-elles pour autant s'en remettre aux déclarations des prestataires étrangers dont l'intérêt est précisément de conquérir leur clientèle ? Non, et les clients doivent disposer d'une appréciation propre de la conformité du droit local.

L'analyse doit prendre en compte toutes les étapes du traitement : plus nombreux sont les acteurs qui participent au transfert ou au traitement transféré, plus complexe devient alors l'analyse. Cette étude doit être menée en considération des caractéristiques du traitement, car elles peuvent toutes activer des législations locales spécifiques :

- Finalités poursuivies (gestion des ressources humaines, marketing, support IT, profilage de consommateurs, publicité digitale, essais cliniques…) ;
- Type d'entités impliquées (publiques ou privées, responsable de traitement ou sous-traitant, responsable conjoint ou sous-traitant ultérieur…) ;
- Secteur en cause (télécoms, finances, santé, adtech, commerce…) ;
- Catégories de données personnelles transférées (ex : données RH, données clients, données sensibles, données de mineurs, etc.) ;
- Format de transfert des données (en clair, pseudonymisées, chiffrées…) ;
- Possibilité que les données fassent l'objet d'un transfert *ultérieur* vers un troisième pays, etc.

L'analyse de la loi locale doit évidemment porter sur les textes applicables, mais aussi sur l'existence et la nature des recours juridictionnels qui sont prévus au bénéfice des personnes

[5] Sauf si le transfert entre dans les exceptions prévues à l'article 49 RGPD, par exemple pour des transferts ponctuels.

[6] « *you must assess, where appropriate in collaboration with the importer, if there is anything* ***in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards*** *of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer* »

[7] « *your data importer should provide you with the relevant sources and information relating to the third country in which it is established and the laws applicable to the transfer. You may also refer to other sources of information* ».

physiques elles-mêmes y compris contre un accès aux données par une autorité publique, l'existence d'une législation spécifique de protection des données, l'existence d'une autorité de contrôle…

On le voit, le travail d'analyse juridique exigé des entreprises françaises et européennes est titanesque, et en pratique, hors de portée de la plupart d'entre elles. Pourquoi formuler de telles exigences lorsqu'il est patent que même les grands groupes ne pourront y sacrifier ? Que valent des recommandations qui ont de grandes chances de rester absolument théoriques ?

Le CEPD renvoie ensuite à une seconde recommandation du 10 novembre 2020, n°02/2020 intitulée « *Garanties Essentielles Européennes* », émise pour compléter la recommandation 01/2020 sur les mesures additionnelles, et qui identifie d'autres éléments à prendre en compte (agences nationales de sécurité ou de renseignement, disponibilité, clarté et non-ambiguïté des règles d'accès aux données par les autorités locales, etc.). Cette seconde recommandation du CEPD doit permettre de déterminer si la loi locale prévoit des accès aux données justifiables ou non, et si elle peut contredire les engagements contractuels de l'importateur de données.

2.6 Le respect des garanties essentielles européennes

Le CEPD avait œuvré à la définition de ces principes dès l'invalidation du *Safe Harbor*, afin de dégager les règles que toute législation étrangère doit respecter pour pouvoir être reconnue comme compatible avec la législation européenne de protection des données personnelles, en s'appuyant sur la jurisprudence de la CJUE et de la CEDH, en application de la Charte des droits fondamentaux et de la Convention européenne des droits de l'homme.

La décision *Schrems II* a été l'occasion pour le CEPD d'actualiser ses travaux, desquels il ressort que :

- Les droits fondamentaux des personnes incluent notamment le respect de leur vie privée et familiale, y compris leurs communications, et la protection de leurs données personnelles ;
- Une ingérence (par un gouvernement étranger par exemple) dans ces droits fondamentaux n'est possible que si elle procède d'un autre impératif majeur exprimé par la loi, ne porte pas atteinte à l'essentiel des droits fondamentaux, et reste proportionnée et assortie de recours effectifs et impartiaux. Nous retenons ce terme d'« ingérence » ci-après pour viser les accès ou divulgations de données auprès des autorités étrangères (juges, gouvernements, services de police ou de renseignement) ;
- Le droit européen pose quatre garanties incontournables permettant de déterminer si une ingérence (par exemple des autorités publiques ou des services de renseignement d'un pays) est acceptable, ou disproportionnée.

Les quatre garanties essentielles européennes sont les suivantes :

- **Licéité de l'ingérence** : l'ingérence (l'accès et l'utilisation ultérieure des données par l'autorité étrangère) doit reposer sur des règles claires, précises et accessibles, définies au sein d'une loi qui définit les circonstances, motifs et limites de l'ingérence, exclusive de toute forme d'abus ou d'arbitraire. Il s'agit ici du principe classique selon lequel une atteinte ne peut être imposée à un droit fondamental que si elle est strictement justifiée

par le législateur souverain[8]. A titre d'exemple, les règles d'interception de conversations téléphoniques ou de correspondances électroniques doivent être justifiées par une loi (et cette loi doit respecter des principes fondamentaux, comme la France l'a appris à ses dépens devant la CJUE qui a condamné sa conservation indifférenciée des données de connexion dans un arrêt du 6 octobre 2020) ;

- **Nécessité et proportionnalité de l'ingérence** : l'atteinte à un droit fondamental doit être strictement nécessaire à l'objectif poursuivi, et proportionnée. Ces critères s'apprécient au regard de l'importance de l'objectif d'intérêt général qui fonde l'ingérence : sauvegarde de la sécurité nationale, lutte contre le terrorisme, etc. Seules les données nécessaires et proportionnées à cet impératif doivent pouvoir être collectées[9].
- **Mécanisme de surveillance indépendant** : l'accès aux données doit être soumis à la surveillance d'un juge ou d'un autre organe impartial (tel qu'une autorité administrative indépendante). A titre d'exemple, l'accès ou l'interception des données doit procéder de la décision d'un magistrat indépendant, et le dispositif d'interception lui-même ne doit permettre que ce qui a été autorisé par le magistrat. Cette indépendance exclut tout organe seulement politique ou émanant du seul exécutif local, ainsi bien entendu que tout conflit d'intérêts ;
- **Voies de recours effectives** : outre la surveillance de l'ingérence par une autorité indépendante, la quatrième garantie essentielle réside dans la faculté pour les personnes concernées d'introduire elles-mêmes un recours en cas d'atteinte injustifiée à leurs droits, et donc à la confidentialité de leurs données. L'existence de voies de recours effectives, indépendantes et accessibles est un pilier des états de droit, il n'est donc pas étonnant qu'on retrouve ici cette exigence. Ce recours doit permettre notamment à la personne concernée d'accéder aux données interceptées, demander leur suppression ou s'opposer à l'ingérence. En bonne logique, la CJUE a rappelé que la personne devait donc être informée de ladite ingérence (sauf si une telle information ruine le motif d'intérêt général pour lequel l'ingérence est mise en œuvre…).

Pour illustrer cette dernière garantie essentielle, la CJUE a indiqué dans l'affaire *Schrems II* que le « médiateur » prévu par le *Privacy Shield* américain ne présentait pas les caractéristiques d'une autorité impartiale, indépendante et experte dignes d'une véritable juridiction.

Ainsi, dans le cadre de l'étude de la législation du pays vers lequel sont exportées les données, telle qu'imposée par le CEPD dans sa recommandation n°01/2020, les cocontractants doivent vérifier si cette législation prévoit (i) des possibilités d'ingérence, encadrées par la loi et justifiées par un intérêt public supérieur, (ii) le caractère strictement nécessaire et proportionné de l'ingérence, (iii) la surveillance de l'ingérence par une autorité indépendante et (iv) des voies de

[8] Ce même principe explique également les condamnations prononcées par la CJUE contre les législations européennes qui prévoient une collecte et conservation indifférenciée et indiscriminée des données de communications électroniques, à la suite des affaires *Digital Rights Ireland* (CJUE 8 avril 2014, aff. jointes C-293/12, C-594/12) et *Tele2 Sverige* (21 décembre 2016, *Tele2 Sverige AB*, aff. C-203/15), ainsi plus récemment que les décisions Privacy International (CJUE 6 octobre 2020, aff. C-623/17) et Quadrature du Net, FDN et Ordre des barreaux francophones et germanophones, CJUE 6 octobre 2020 aff. jointes C-511/18, C-512/18, C-520-18)

[9] Le CEPD rappelle en particulier que selon la CJUE elle-même, une « *réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée* », et doit toujours « *répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi* ».

recours effectives et impartiales permettant à la personne concernée de s'opposer à ladite ingérence et de protéger ses données personnelles de manière effective[10].

L'analyse doit aussi se nourrir d'autres sources, et notamment, vérifier si le pays tiers peut chercher à accéder aux données *à l'insu même* de l'importateur de données au regard d'éventuels précédents, ou encore si ce pays pratique les interceptions techniques de données sur ses télécommunications. Il ne s'agit donc même plus d'une analyse exhaustive du droit étranger sous l'angle des interceptions légales, mais aussi d'une analyse des pratiques gouvernementales ou des agences de renseignement, qui par construction sont le plus souvent occultes…

Dans sa recommandation, le CEPD prend l'exemple concret des requêtes FISA aux USA, qui ne répondent pas aux exigences de proportionnalité du RGPD. A cet égard, le CEPD confirme noir sur blanc le fait que, dans le cas des USA au moins, les CCT comme les BCR ne suffisent plus pour autoriser les transferts de données aux prestataires US, même s'ils utilisent des datacenters européens.

Cette analyse juridique doit permettre de conclure soit (i) à la confirmation du caractère effectif des garanties déployées pour encadrer le transfert, compatibles avec les garanties essentielles européennes, soit (ii) au contraire, à l'infirmation de ce caractère effectif, et dans ce cas, à la nécessité de mettre en place des mesures additionnelles… ou de cesser tout transfert.

2.7 Adopter des mesures additionnelles

Si l'analyse juridique menée (pour autant qu'elle soit faisable…) constate que les quatre garanties essentielles européennes ne sont pas établies au sein du pays importateur des données, il faut alors identifier, en concertation avec l'importateur de données, les mesures additionnelles qui aplaniront les incompatibilités détectées. Ces mesures peuvent être de nature contractuelle, technique et/ou organisationnelle, et il s'agira souvent d'une *combinaison* de mesures.

Le CEPD indique dans sa recommandation n°01/2020 que des engagements contractuels complémentaires seront souvent insuffisants pour empêcher la possibilité d'un accès abusif aux données par les autorités du pays tiers. Il y a donc des situations dans lesquelles seules des mesures *techniques* constitueront une solution décisive, en créant des obstacles réels et définitifs aux accès non autorisés[11]. Rarement l'adage « *code is law* » de Laurence Lessig aura été mieux illustré qu'ici.

[10] Le CEPD écrit que « *Les garanties essentielles européennes mises à jour ont pour but de fournir des éléments permettant de déterminer si des mesures de surveillance autorisant l'accès d'autorités publiques d'un pays tiers à des données à caractère personnel, qu'il s'agisse d'agences de sécurité nationale ou d'autorités répressives, peuvent être considérées comme une ingérence justifiable ou non*. », mais précise que ces garanties essentielles « *ne visent pas, en soi, à définir tous les éléments qu'il conviendrait de prendre en considération pour apprécier si le régime juridique d'un pays tiers empêche l'exportateur et l'importateur des données de fournir des garanties appropriées conformément à l'article 46 du RGPD*. »

[11] *« there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes »*

Ce n'est qu'une fois les mesures déployées et la protection rétablie conformément aux exigences du RGPD, que le traitement peut être mis en œuvre.

A défaut de mesures additionnelles efficaces, ou si elles sont interdites dans le pays destinataire (ex : interdiction de la cryptographie), le transfert est alors considéré comme illicite et il ne peut pas y être procédé. D'ailleurs, le CEPD souligne que le transfert doit être suspendu pendant l'analyse de compatibilité juridique et jusqu'au déploiement des mesures additionnelles. Si le responsable de traitement poursuit le transfert en l'absence de ces précautions, il doit alors le notifier à l'autorité de contrôle comme prescrit par l'article 46 RGPD, qui décidera du sort du transfert.

En pratique, la plupart des flux de données vers des prestataires étrangers devrait donc être signalés par les entreprises françaises à la CNIL, dans la mesure où les analyses juridiques de compatibilité n'ont pas encore été menées, ni aucune mesure additionnelle véritablement déployée. On mesure ici à quel point la situation réelle est éloignée des recommandations du CEPD.

Pourtant, cette illicéité des flux transfrontaliers qui se poursuivraient en l'absence de l'analyse de compatibilité juridique et du déploiement de mesures additionnelles a été confirmée par la CNIL en France, dans le cadre de recours introduits contre la décision du « *Health Data Hub* » de s'appuyer sur des services fournis par l'éditeur américain Microsoft. Devant le Conseil d'Etat, la CNIL a transmis un mémoire dans lequel elle concluait que même en cas d'hébergement des données par Microsoft uniquement sur le territoire européen, et même en cas d'interdiction d'accès à Microsoft aux fins de maintenance du système, les prérogatives du gouvernement américain pouvaient toujours conduire Microsoft à devoir répondre à ses injonctions et lui donner accès aux données, y compris en permettant leur déchiffrement le cas échéant.

La CNIL a confirmé que de telles injonctions des autorités US doivent être considérées comme des *divulgations non autorisées* par le RGPD (art. 48), et que les données personnelles des européens, tout particulièrement les données personnelles de santé, doivent être soustraites aux prérogatives des autorités américaines.

En conséquence, « *cette situation doit conduire* » selon la CNIL « *à modifier les conditions d'hébergement de la plateforme, ainsi que celles des autres entrepôts de données de santé qui sont hébergés par des sociétés soumises au droit étatsunien. La solution la plus effective consiste à confier l'hébergement de ces données à des sociétés non soumises au droit étatsunien* ». Et ce changement d'hébergement « *devrait intervenir dans un délai aussi bref que possible* ».

Si le sujet légitimement sensible des données de santé des français a justifié cette prise de position de la CNIL, cette position est en réalité applicable à tous types de données à caractère personnel. Il ne fait donc plus de doute à ce jour que les entreprises doivent impérativement mettre en œuvre les études juridiques de compatibilité des législations étrangères avec le RGPD, et convenir avec leurs prestataires des mesures additionnelles à déployer pour mettre les données des européens à l'abri de toute ingérence qui ne répondrait pas, a minima, aux quatre garanties essentielles analysées supra.

2.8 Exemples de mesures additionnelles donnés par le CEPD

Devant ces considérations juridiques angoissantes, les entreprises françaises et européennes sont en attente de solutions pratiques. Le CEPD a donc souhaité proposer des cas pratiques, à titre d'illustration. Mais le CEPD souligne qu'il n'est pas question de déployer un ou plusieurs de ces exemples *ex nihilo* ; la pertinence et l'efficacité des mesures additionnelles déployées sera nécessairement établie par rapport aux failles et risques identifiés dans la phase amont d'analyse du contexte réglementaire et pratique du transfert et de l'importateur de données.

Mesures techniques. Outre l'accès direct aux données, le CEPD indique que les mesures doivent « *empêcher les autorités d'identifier les personnes concernées, en déduisant des informations à leur sujet, en les distinguant dans un autre contexte ou en associant les données transférées à d'autres ensembles de données qu'ils peuvent posséder et pouvant contenir, entre autres données, des identifiants en ligne fournis par les dispositifs, applications, outils et protocoles utilisés par les personnes concernées dans d'autres contextes.* ».
Les mesures doivent prendre en compte le fait que les accès illicites des autorités étrangères peuvent porter sur les lignes de télécommunications utilisées pour convoyer les données vers le pays destinataire (interceptions techniques), ou directement sur les serveurs et datacenters exploités par les prestataires étrangers.

Le CEPD évoque plusieurs cas de figure, selon que l'hébergement des données implique ou n'implique pas qu'elles soient accessibles « en clair », selon que les données sont pseudonymisées, selon qu'elles transitent par un troisième pays, selon qu'elles sont envoyées à un sous-traitant ou à un autre responsable de traitement autonome, etc. Il n'est pas utile de revenir ici sur l'ensemble des mesures techniques qui sont exposées dans la casuistique du CEPD, la principale étant le chiffrement des données d'une façon qui ne permet pas à l'importateur des données de pouvoir les déchiffrer[12] ni de réidentifier les personnes via d'autres moyens.

Mesures organisationnelles. Là encore, il convient de se référer à la casuistique proposée par le CEPD : politiques internes de gouvernance des flux de données, formation renforcée des personnels qui manipulent les données, documentation et suivi des demandes d'accès reçues des autorités du pays étranger, publication de rapports périodiques sur les demandes gouvernementales, minimisation systématique des données transférées, etc. : ces mesures organisationnelles dépendant largement de la nature des données et du contexte particulier des traitements.

Mesures contractuelles. Enfin et surtout, le CEPD a évoqué des mesures additionnelles à mettre en œuvre au niveau juridique. Elles ont souvent pour objet rendre contractuelles les mesures techniques ou organisationnelles évoquées ci-avant. Au titre de ces mesures additionnelles de nature *contractuelle*, le CEPD a listé les exemples suivants :

- **Engagement d'implémenter des mesures additionnelles techniques et/ou organisationnelles** qui mettent définitivement les données à l'abri de toute divulgation

[12] C'est d'ailleurs l'un des rappels formulés par la CNIL devant le Conseil d'Etat : si le prestataire qui traite des données chiffrées est soumis à un droit incompatible avec le RGPD, mais que le prestataire lui-même détient la clé de déchiffrement, alors il peut l'utiliser pour en permettre l'accès, en clair, aux autorités du pays d'accueil.

non conforme au RGPD : il convient que les cocontractants déterminent ensemble, éventuellement sur proposition du prestataire, les mesures techniques ou organisationnelles pertinentes pour réduire ou éliminer les risques d'accès des autorités publiques étrangères aux données, en fonction de la nature de celles-ci et des utilisations qui en sont faites (on retrouve ici l'approche par le risque) ;

- **Engagement d'informer le client des accès aux données** que les autorités du pays tiers souhaiteraient obtenir, ce qui peut impliquer de lister les lois et règlements locaux qui permettraient l'ingérence des autorités locales, mais aussi de fournir des informations et statistiques basées sur le vécu du prestataire (reçoit-il souvent des requêtes FISA du gouvernement US ? Combien de fois par an ? Quelles réponses y sont apportées ? Quelles données sont visées ? Etc.) ou des rapports provenant de sources officielles et fiables (open source, jurisprudence nationale, organismes de surveillance, etc.) portant sur les requêtes généralement formulées par les autorités locales. Cet engagement d'information peut également consister à décrire quelles mesures sont en place pour empêcher l'accès de tout tiers aux données transférées, décrire les détails des accès que le prestataire a précédemment permis aux autorités locales au cours d'une période déterminée, etc. ;
- **Engagement de signaler les modifications de la législation du pays d'importation des données** : si la législation locale était initialement considérée comme offrant un niveau de protection équivalent au RGPD, mais que cette législation évolue, le prestataire s'engage à informer le client de son incapacité désormais d'assurer la protection des données, du fait de cette évolution de son environnement juridique. Cela implique nécessairement que la notification soit faite avant l'accès aux données des autorités locales, que le prestataire assure la veille juridique des évolutions de son droit national pour pouvoir signaler les changements, et que le contrat prévoie un mécanisme permettant au client de sécuriser ou récupérer rapidement ses données – voire de cesser de recourir au prestataire si rien d'autre ne peut être fait pour atténuer les effets de la modification réglementaire locale ;
- **Engagement d'audit** : le client peut renforcer ses droits d'audit et d'inspection sur les installations de traitement des données du prestataire de nationalité étrangère, afin de vérifier si les données ont pu être divulguées aux autorités locales et si oui dans quelles conditions, ce qui implique la faculté d'auditer les installations et systèmes et d'accéder aux journaux de logs – audits que refusent cependant les grands cloud providers notamment américains, pour des raisons de maintien de la sécurité… ;
- **Engagement de transparence** : le contrat peut renforcer les obligations de transparence du prestataire en prévoyant ce que le CEPD appelle un "*warrant canary*", par lequel il est tenu de publier régulièrement (ex : tous les jours) un message chiffré électroniquement informant le client qu'il n'a reçu aucun ordre de divulguer des données personnelles ; l'absence de réception de cet avis quotidien alerterait donc le client, sans que le prestataire ait à violer une interdiction d'alerte qui lui est imposée par son droit national… ;
- **Interdiction de toute « backdoor »** : le contrat peut stipuler une clause exigeant que le prestataire certifie que (a) il n'a pas délibérément créé au sein de sa solution informatique de porte dérobée qui pourrait être utilisée par une autorité étrangère pour accéder aux données ; (b) il n'a pas délibérément créé ou modifié ses processus commerciaux pour faciliter l'accès aux données ; et (c) que la législation nationale ou la politique gouvernementale locale n'exige pas du prestataire qu'il facilite l'accès aux

données. Mais cela suppose que la législation locale n'interdise justement pas à ce prestataire de divulguer de telles informations… ;

- **Engagement de contester la légalité de la demande d'accès émanant d'une autorité** : le prestataire s'engage à examiner la légalité de la demande d'accès aux données émanant d'une autorité locale, jusqu'à contester l'ordre si possible, et s'engage également à ne fournir que le minimum d'informations possible lorsqu'il est contraint de répondre à la demande d'accès – mais là encore cela suppose que la législation du pays tiers autorise ce prestataire à contester l'ordre de communication des données… ;
- **Engagement d'alerte** : le prestataire peut s'engager à informer l'autorité locale requérante de l'incompatibilité de sa demande d'accès avec les garanties convenues avec ses clients (dont les CCT) : dans ce cas, le prestataire devrait notifier simultanément son client et l'autorité de contrôle compétente de l'Union Européenne. Mais comme précédemment, cela n'est efficace que si la loi locale donne un effet à de telles contestations et n'interdit pas la notification aux clients ou aux CNIL européennes… ;
- **Engagement de donner aux personnes concernées le droit de consentir au préalable à la divulgation de leurs données** : ici, le contrat entre client et prestataire peut prévoir que les données transférées en clair ne sont accessibles qu'avec le consentement exprès ou implicite du client ou de la personne concernée, ce qui là aussi a très peu de chances d'être efficace si la loi locale n'autorise pas le prestataire à déconfidentialiser l'ordre d'accès, sauf si l'autorité publique accepte de renoncer à cet accès si la personne concernée s'y oppose (ce qui n'est pas le cas pour les réglementations de surveillance globale des USA). De plus, on imagine assez mal les entreprises européennes autoriser leurs prestataires américains à contacter directement leurs salariés, prospects ou clients finaux pour les alerter d'un accès demandé par un juge américain, compte tenu de la perte de confiance qu'une telle alerte engendrerait… sans oublier que la plupart des sous-traitants préfèrent laisser aux responsables de traitement l'exclusivité des relations avec les personnes concernées ;
- **Engagement d'assistance aux personnes concernées** : ici, le contrat entre client et prestataire peut les engager à aider la personne concernée à exercer ses droits devant la juridiction compétente du pays tiers par le biais de mécanismes de recours ad hoc et de conseils juridiques locaux – ce qui implique qu'existe une juridiction reconnue comme telle dans le pays concerné (pour mémoire, la CJUE a considéré que le médiateur désigné dans le *Privacy Shield* ne répondait pas à l'exigence d'indépendance de la juridiction), etc.

Le CEPD précise, sous chaque exemple de mesure additionnelle proposé, les conditions de son efficacité. La recommandation 01/2020 du CEPD constitue donc une *boîte à outils*, qui suggère des mesures additionnelles de nature technique, organisationnelle et/ou contractuelle, parmi lesquelles les cocontractants peuvent choisir celles qui permettraient de manière *effective* d'empêcher l'accès aux données par des autorités locales, même si cet accès est prévu par les lois locales.

Or, ces mesures sont parfois très théoriques, et beaucoup de directions juridiques peinent à imaginer comment les mettre en œuvre dans le contexte des nombreux contrats qui confient les données personnelles d'européens à des prestataires étrangers dont le droit national ne garantit pas de protection adéquate. En particulier dans les cas où le CEPD indique lui-même qu'aucune mesure effective n'est imaginable, comme lorsque les données

doivent être traitées à distance *mais en clair*, ou lorsque le sous-traitant étranger a nécessairement besoin de voir les données en clair pour exécuter ses prestations.

En toute hypothèse, cconformément aux logiques de « compliance » et d'accountability qui caractérisent le RGPD, les mesures additionnelles qui seront choisies et mises en œuvre devront également pouvoir évoluer en fonction de l'évolution des traitements, des finalités, ou du contexte légal et réglementaire du pays étranger en cause, mais aussi du « risque » que les traitements entraînent pour les personnes concernées.

C'est cette approche par le risque, qui préside déjà à l'exécution des analyses d'impact (AIPD), qui est le plus souvent adoptée à ce jour : en fonction de la criticité des données (ex : données de santé, profilage des personnes, etc.), et en fonction de la criticité des traitements pour l'entreprise, celle-ci doit faire le choix de renforcer l'encadrement des transferts le mieux possible, ou de renoncer aux dits transferts.

En conséquence, on commence à rencontrer de nouvelles clauses dans les contrats conclus entre des entreprises françaises et leurs cocontractants étrangers, notamment américains, dans lesquelles ces derniers s'engagent par exemple à :

- Prévenir le client de manière réactive et par écrit, dans le cas où ils recevraient une demande d'accès émanant de l'autorité locale, et préciser les détails de cette demande et les données visées (sous réserve que la loi locale autorise le prestataire à le faire…) ;

- Se concerter avec le client pour identifier si des objections peuvent être opposées à la demande d'accès, en invoquant les exigences du RGPD dont est tenu le prestataire (ou d'autres réglementations telles que le secret des correspondances ou la loi n°68-678 du 26 juillet 1968 dite « loi de blocage » qui régit la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères). Certaines clauses visent d'ailleurs expressément les requêtes FISA ou l'Executive Order 12333 mentionnés par la décision de la CJUE dans l'affaire *Schrems II*), ou le CLOUD Act américain ;

- Introduire tout recours permettant d'empêcher ou réduire l'accès demandé, et informer régulièrement le client de l'évolution de ce recours (toujours sous la réserve que la loi étrangère prévoie ce genre de recours…) ;
- Accepter une éventuelle décision de résiliation du contrat, si le client estime qu'il n'a pas d'autre moyen d'empêcher l'accès aux données par les autorités locales, etc. – ce qui est bien plus difficile à faire accepter à un prestataire qui verra lui échapper une part significative de son revenu sans qu'il ait commis de faute…

On souligne au passage que demander aux prestataires de s'engager à soustraire les données des européens au contrôle des autorités étrangères, *sous réserve que les lois étrangères elles-mêmes le permettent*, est un raisonnement circulaire qui ne résout rien.

Les exemples donnés par le CEPD ne sont justement que des exemples. Il appartient aux parties de déterminer en concertation la meilleure combinaison possible de mesures techniques, organisationnelles et contractuelles permettant d'empêcher l'accès des autorités étrangères aux données. Il s'agit du reste de la philosophie globale du RGPD, qui impose une « co-

responsabilité » des responsables de traitements et de leurs sous-traitants dans la protection des données, mais leur laisse la responsabilité de définir et déployer les « *mesures techniques et organisationnelles appropriées* ».

La stupeur passée, le marché a attendu dans un premier temps les engagements complémentaires qu'allaient proposer les prestataires américains. Or, de nombreux prestataires se disent désemparés, pris entre deux feux : d'un côté leurs clients européens soumis au RGPD, dont ils ne doivent plus pouvoir communiquer les données si leur gouvernement les demande, et de l'autre, leur gouvernement qui entend faire appliquer ses lois locales, et accéder à toute donnée s'il estime que cet accès est nécessaire en particulier pour assurer sa sécurité nationale.

Des engagements complémentaires d'alerte, de réactivité, d'information ont donc commencé à fleurir dans les contrats, sans pour autant qu'on puisse considérer que ces engagements permettent effectivement d'empêcher toute ingérence. Les prestataires étrangers, américains en particulier, prennent soin de rappeler qu'ils ne sauraient résister aux injonctions légales de leurs gouvernements, ce qui est bien compréhensible.

C'est dans ce contexte que la Commission européenne a confirmé la publication de nouvelles clauses contractuelles types (CCT), contemporaines du RGPD et censées embarquer également des réponses juridiques à la situation cornélienne décrite ci-avant.

3. LES NOUVELLES CCT DE LA COMMISSION EUROPEENNE DU 4 JUIN 2021

Le 4 juin 2021, la Commission européenne a adopté ces nouvelles CCT portant sur les transferts de données personnelles vers un pays tiers, qui viennent remplacer les CCT précédentes (qui dataient de 2004 pour les CCT entre responsables de traitement, et de 2010 pour les CCT entre un responsable de traitement et un sous-traitant).

Ces nouvelles CCT sont rédigées sous forme de modules pour épouser plusieurs contextes (entre responsables de traitement autonomes, entre un responsable de traitement et son sous-traitant, entre un sous-traitant et une sous-traitant ultérieur…), ce qui implique de qualifier les protagonistes du transfert pour pouvoir choisir quel module adopter et annexer au contrat de services.

Ces nouvelles CCT actent de l'entrée en vigueur du RGPD et en intègrent les grands principes. Elles rappellent les droits dont disposent les personnes concernées et indiquent les modalités d'exercice de ces droits, y compris directement auprès du prestataire importateur de données. Ces CCT visent également à renforcer la transparence pour les personnes concernées, notamment en leur fournissant copie des CCT signées. Elles intègrent également l'opportunité de recourir à des mesures de pseudonymisation et de chiffrement, en fonction des risques auxquels sont exposées les personnes concernées.

Ces nouvelles CCT imposent à l'exportateur et à l'importateur de données de conserver les preuves de leur conformité au RGPD à tout moment (*accountability*) et donc conserver la trace des activités effectuées sur les données.

Elles restreignent également la possibilité de transferts ultérieurs, le second importateur devant nécessairement se conformer aux CCT ou être sis dans un pays de législation adéquate. Il est également possible de permettre à ce sous-traitant ultérieur ou ce tiers destinataires de s'amarrer aux clauses contractuelles types, en en devenant signataire à son tour – ce qui crée alors une relation directe entre le client en début de chaine contractuelle, et le sous-traitant ultérieur, relation directe qui contredit des stipulations usuellement prévues qui rendent le prestataire seul responsable devant le client des éventuels manquements de ses sous-traitants… Mais à défaut d'un tel amarrage, seul le consentement explicite et éclairé des personnes concernées permettrait alors un tel transfert ultérieur.

Enfin, ces nouvelles CCT organisent la responsabilité des acteurs pour chaque type de transfert de données. Mais surtout, leurs nouveaux articles 14 et 15 visent à prendre en compte les conséquences de l'arrêt *Schrems II* :

L'article 14 des CCT dispose que « *Les parties garantissent qu'elles n'ont aucune raison de croire que la législation et les pratiques du pays tiers de destination applicables au traitement des données à caractère personnel par l'importateur des données, notamment les exigences en matière de divulgation de données à caractère personnel ou les mesures autorisant l'accès des autorités publiques à ces données, empêchent l'importateur de données de s'acquitter des obligations qui lui incombent en vertu des présentes clauses (..)* ».

Les clients européens, exportateurs de données, s'efforceront ici de faire peser sur le prestataire, importateur de données, la responsabilité de mener l'analyse du droit applicable (et des pratiques des autorités locales…). Mais la démarche est périlleuse, car comme rappelé ci-avant, c'est au client que revient en premier lieu de mener l'analyse du droit étranger au regard des « *Garanties Essentielles Européennes* » du droit européen. Concrètement, les deux parties devront pouvoir montrer qu'elles ont œuvré ensemble à cette analyse et à la détermination de la compatibilité ou l'incompatibilité du droit local avec le RGPD.

Au-delà, le prestataire devra, s'il a des raisons de croire qu'il est ou sera soumis à une législation ou pratique non conforme, prévenir le client. Suite à cette notification ou si le client a des raisons de croire que son prestataire ne peut plus s'acquitter de ses obligations, le client devra définir des mesures appropriées en vue de remédier à la situation, ou faire cesser le transfert. On pressent déjà les conséquences complexes en cas de désaccord entre client et prestataire sur l'incompatibilité d'une évolution législative étrangère…

L'article 15 des CCT prévoit quant à lui de nouvelles obligations à la charge du prestataire importateur de données en cas d'accès aux données par les autorités de son pays. En cas de requête obligeant ce dernier à fournir un accès aux données, ces nouvelles CCT l'obligent à (i) informer l'exportateur de données, (ii) à fournir aux autorités de contrôle européennes un maximum d'informations sur cette demande (nombres de demandes, types de données demandées, autorité requérante, etc..) et (iii) à déployer ses meilleurs efforts pour limiter cet accès ou en obtenir la levée - ce qui accroît considérablement les charges des prestataires et risque, malheureusement pour leurs clients européens, d'avoir un impact sur les prix.

L'importateur de données doit également contrôler la légalité de l'ordre d'accès formulé par les autorités du pays d'importation, afin de vérifier si l'ordre est conforme aux pouvoirs desdites autorités, et contester cet ordre le cas échéant.

Selon le considérant 24 de la décision d'exécution (UE) 2021/914 relative aux nouvelles CCT, elles abrogeaient les anciennes dès la fin septembre 2021 et s'imposent pour tout nouveau contrat négocié à compter de cette date. Elles prévoient toutefois la survie provisoire des anciennes CCT pendant 15 mois à compter de septembre 2021, mais seulement si les contrats préexistaient, si les traitements sont inchangés, et si les anciennes CCT suffisent à garantir la protection des données contre les divulgations - donc en pratique, ce délai complémentaire semble illusoire dès lors que les transferts sont effectués vers un pays dont nous savons que la loi locale pose problème, à l'instar des USA.

En substance, on retrouve donc dans les CCT un grand nombre des recommandations précédemment émises par le CEPD, qui sont désormais incontournables, et qui vont significativement alourdir les obligations des entités importatrices de données (qu'elles soient des filiales ou des sous-traitants à l'étranger). Un réflexe doit donc être, a minima, d'imposer les CCT de juin 2021 dans tout contrat négocié par un client français avec un prestataire étranger ou dont les sous-traitants étrangers relèvent de pays dont la législation n'est pas reconnue par la CNIL comme équivalente au RGPD.

4. LES INITIATIVES DU MARCHE FACE AU NOUVEAU CONTEXTE JURIDIQUE

Devant cette situation assez inextricable sur le plan juridique, et afin de sauvegarder le plus possible aujourd'hui et demain les échanges économiques et le recours aux outils technologiques proposés par des prestataires extra-européens, diverses initiatives ont vu le jour avec plus ou moins de bonheur.

En mai 2021, le gouvernement a présenté un « label de confiance » consacré au « *cloud souverain français* », incarné par une certification technique délivrée par l'ANSSI : SecNumCloud[13]. Ce label était présenté comme réunissant l'ensemble des exigences de sécurité technique, conforme aux meilleures pratiques en vigueur, mais aussi aux exigences de protection des données personnelles contre les possibilités d'ingérence, de la part des autorités étrangères (dont les USA). Il s'agit là de premières précautions que les DSI des entreprises françaises seraient avisées d'adopter, outre la référence aux meilleures normes et standards du marché telles qu'ISO 27001.

L'ANSSI vient d'ailleurs d'actualiser ce label pour mieux tenir compte de l'enjeu mis à jour par la CJUE, en indiquant que le client et le prestataire doivent préciser, dans leur convention de service, *« que la collecte, la manipulation et le stockage des données faits dans le cadre de l'avant-vente, de la mise en œuvre, de la maintenance et l'arrêt du service sont conformes aux exigences*

[13] https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf

édictées par la législation française et européenne en vigueur et que ces mêmes données ne sont pas soumises à d'autres régimes juridiques ».

Pour autant, ce label n'est pas un sauf-conduit, puisque l'ANSSI rappelle qu'il *« n'apporte pas de garanties techniques fortes contre un accès du prestataire aux données traitées sur le système d'information du service, uniquement des engagements contractuels. Les commanditaires souhaitant assurer la protection, sur le plan technique, de leurs données contre un accès par le prestataire, devront par conséquent mettre en œuvre des moyens complémentaires de chiffrement, sous leur maîtrise, de leurs données. »*

L'ANSSI propose à cet égard que le prestataire qui est soumis à une législation étrangère doit lister *« dans un document spécifique, les risques résiduels liés à l'existence de lois extraterritoriales ayant pour objectif la collecte de données ou métadonnées des commanditaires sans leur consentement préalable » et « mettre à la disposition du commanditaire, sur demande de celui-ci, les éléments d'appréciation des risques liés à la soumission des données du commanditaire au droit d'un état non-membre de l'Union européenne ».*

Sur le plan juridique, le label SecNumCloud impose que *« le siège statutaire, administration centrale ou principal établissement du prestataire doit être établi au sein d'un Etat membre de l'Union européenne. Le capital social et les droits de vote dans la société du prestataire ne doivent pas être, directement ou indirectement : individuellement détenus à plus de 24 % et collectivement détenus à plus de 39 % par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un État non membre de l'Union européenne ».*

En parallèle des annonces gouvernementales, de nouveaux partenariats ont été annoncés, notamment la joint-venture « *Bleu* » fruit de la coopération entre Microsoft, Capgemini et Orange, permettant la commercialisation en Europe de la suite Microsoft 365 et du cloud Azure, dans un premier temps à destination des OIV et administrations françaises, mais à terme à toutes les entreprises désireuses de continuer à utiliser les technologies Microsoft (ou qui n'ont techniquement pas d'autre choix).

Cette stratégie vise à mettre en place un bouclier de protection, non plus aux USA, mais directement en Europe, en contraignant les acteurs économiques étrangers à recourir à des acteurs européens du secteur numérique.

Schématiquement, il est question de favoriser la commercialisation d'offres logicielles américaines (Microsoft, Amazon, Google, etc.) par des entreprises françaises ou européennes qui prendront elles-mêmes en charge l'hébergement des données. Il s'agit d'un moyen de conserver la maîtrise des données transmises à des entreprises qui ne sont ni localisées sur le territoire américain, ni légalement soumises aux lois américaines. Cela implique la conclusion de licences de distribution entre les acteurs américains et les hébergeurs européens, ces derniers devenant des distributeurs des technologies américaines.

Cette stratégie reprend et systématise des initiatives qui avaient été prises isolément, notamment par Google qui avait officialisé un partenariat de ce type avec l'hébergeur français OVHCloud dès octobre 2020, portant sur la commercialisation par OVHCloud de la plateforme Anthos. Ici, Google devenait simple éditeur de licences et non plus pleinement cloud provider.

Plus récemment, c'est Thalès qui a annoncé une offre de « *cloud souverain* » en partenariat avec Google.

Cela implique non seulement que les données des clients, dont leurs données personnelles, demeurent strictement hébergées sur le territoire européen, mais que le serveur de licences y soit également, opéré par un prestataire européen, et qu'aucun service ne puisse permettre, même de manière incidente, à l'éditeur américain d'accéder aux données ou de les visualiser, y compris en cas d'intervention de maintenance. Cela conduit donc à confier la maintenance logicielle aux équipes du partenaire européen également, transfert de compétences auxquels tous les éditeurs américains ne sont pas prêts. Et cela pose la question de qui est susceptible d'intervenir sur le code source des services logiciels, car tant qu'il reste sous le seul contrôle de l'éditeur étranger, un risque d'accès subsiste.

Par ailleurs, l'initiative franco-allemande Gaia-X vise également à développer un « *cloud de confiance* » composé d'un écosystème de prestataires européens soumis aux seules lois de l'UE. L'initiative a acquis une dimension européenne. Huit secteurs économiques sont initialement concernés par le projet dont la santé, la finance, le secteur public, l'énergie, la mobilité ou l'agriculture. Mais à ce stade, il s'agit encore d'un projet, d'autant que plus récemment, des cloud providers extra-européens dont AWS, Microsoft, Google, Huawei, Alibaba Cloud et Palantir, ont rejoint Gaia-X. Ce qui en a conduit de nombreux commentateurs à mettre en doute le caractère réellement européen et sécurisé du cloud envisagé… certaines de ces entreprises étant réputées pour le peu de cas qu'elles font, en réalité, des libertés fondamentales.

Gaia-X doit proposer un catalogue de services numériques portés par des hébergeurs et des éditeurs de logiciels préalablement engagés sur des standards « *renforçant la confiance de leurs clients en matière de sécurité des données* » et assurant transparence des contrats. Les fournisseurs de services référencés dans ce projet Gaia-X devront proposer des technologies interopérables d'un hébergeur à l'autre, selon une nomenclature de criticité des données.

Cette idée de licences imposées entre éditeurs américains et hébergeurs européens partait d'une bonne intention : puisque les grands cloud providers américains se taillent une part léonine du marché d'exploitation de la data, de telles licences permettent de ramener vers des entités européennes une partie des chiffres d'affaires réalisés. D'une certaine façon, il est question de rendre des prestataires européens à nouveau bénéficiaires des marchés exploitant les données des européens.

Mais une conséquence de ce projet de constitution d'un « *cloud de confiance* » européen auquel les cloud providers américains sont partie prenante, fût-ce au moyen de licences conclues de gré à gré avec des hébergeurs européens, ou via des options de sécurité et de souveraineté proposées par les prestataires américains (AWS), est paradoxalement qu'un grand nombre d'éditeurs logiciels européens voit la concurrence des américains encore accrue.

Pour ces concurrents européens des services logiciels des prestataires américains, ainsi que pour de nombreux commentateurs, il est inique de parler de « *cloud souverain* » alors que ces offres sont un vecteur complémentaire de pénétration du marché européen pour les éditeurs américains. Ainsi, ce « *cloud de confiance* » fait entrer le loup dans la bergerie et témoigne en réalité d'un manque de soutien à l'industrie européenne, et n'a rien de véritablement « *souverain* ».

D'autres initiatives, telles qu'Euclidia, visent à contourner ces premières critiques, en n'incluant que des fournisseurs strictement européens.

On pourrait certes objecter que la législation de protection des données personnelles, comme les exigences de sécurité de l'ANSSI, n'ont pas pour objet de favoriser tel ou tel secteur de l'industrie, ni de protéger les acteurs français et européens contre leurs concurrents américains ou étrangers, mais d'assurer avant tout la sécurité du patrimoine informationnel des entreprises et la protection des individus. Cela dit, le droit ne s'appréhende pas indépendamment des considérations techniques et économiques qui l'entourent. On comprend donc certains commentaires amers à l'annonce d'un « *cloud de confiance* » aux mains des éditeurs américains !

S'il est évident que ces réglementations sont liées à des enjeux de compétition économique, le « *cloud de confiance* » qu'elles ont vocation à mettre en place est avant tout technique et juridique, et non économique. Et ce, qu'on l'approuve comme de nombreuses DSI désireuses de conserver le bénéfice des technologies de pointe des éditeurs américains, ou qu'on le déplore, comme les éditeurs européens qui y voient non seulement une occasion manquée de favoriser leurs offres, mais aussi une promotion d'autant plus colossale qu'elle est promue par l'Etat, en faveur des éditeurs américains ou d'autres pays étrangers.

Conclusion – Travailler malgré les risques

Depuis le 16 juillet 2020, de très nombreux transferts de données vers des pays tiers, dont les USA, sont devenus *potentiellement* illicites. L'observation du marché montre que certains prestataires d'envergure ont commencé à définir des solutions, mais que la grande majorité s'appuie encore sur les anciennes CCT, ou se contente de déclarations de conformité qui n'engagent que les clients qui souhaitent les croire.

Malheureusement, les diligences à déployer (analyses juridiques des droits étrangers, mesures techniques et contractuelles à négocier avec les prestataires étrangers) sont d'une telle complexité, qu'il est douteux que les clients français puissent rapidement faire disparaître cette non-conformité *potentielle*.

Il est finalement demandé aujourd'hui aux entreprises européennes d'obtenir des engagements des prestataires étrangers que ceux-ci seront le plus souvent dans l'incapacité de prendre compte tenu de leur propre législation nationale. A cet égard, le bras de fer entre Europe et USA entre dans une phase critique. Le pire est que les principes en présence sont parfaitement valables l'un comme l'autre : d'une part la protection des données personnelles contre toute divulgation injustifiée ou à l'insu des personnes ; de l'autre, la protection des individus contre divers réseaux criminels ou terroristes à l'échelle internationale.

Les autorités européennes et américaines ont mis en route, en septembre 2021, de nouveaux pourparlers pour tenter de définir un nouvel accord, qui tirerait les enseignements de l'invalidation du *Privacy Shield* et assurerait aux européens l'existence de véritables recours contre les ingérences du gouvernement ou du juge américain sur leurs données. Mais il est évident qu'une telle négociation prendra de longs mois, d'autant plus qu'en l'absence de cadre

fédéral, certains américains ont voté leur propre législation de protection des données et avancent en ordre dispersé. Et surtout, rien ne garantit qu'un nouveau programme de conformité américain ne serait pas… un nouveau jeu de dupe à l'instar du *Safe Harbor* et du *Privacy Shield*.

Avec la décision de la CJUE de juillet 2020 et les recommandations subséquentes du CEPD, on a atteint donc un point limite de l'application du RGPD, dont le champ est à la fois territorial et personnel. L'ingéniosité des rédacteurs du RGPD résidait en effet dans l'extensivité géographique de cette réglementation souveraine européenne, qui devait suivre les données où qu'elles soient dans le monde et par quiconque les traite.

L'Union Européenne réussissait le tour de force « d'exporter » sa réglementation, ce qui n'a pas manqué d'engendrer des réponses légales d'autres pays, dont les USA, basées sur leurs propres hiérarchies juridiques. L'extensivité du RGPD, et sa confrontation avec les droits nationaux des pays extra-européens, finit par se retourner contre les entreprises européennes, dont on avait pu penser dans un premier temps qu'elles seraient favorisées par la mise en place des plus hauts standards qui soient en matière de protection des données personnelles.

En dehors des décisions d'adéquation prononcées par les autorités de contrôle européennes, ce qui devrait faire l'objet d'accords internationaux bilatéraux ou multilatéraux entre états soucieux de préserver la vie privée et les droits fondamentaux de leurs citoyens, on constate que la question est aujourd'hui délégué aux entreprises elles-mêmes, qui ne disposent pourtant ni des moyens ni des leviers de pression dont disposent les états.

Pour l'heure, la situation est devenue relativement insoluble sur le plan juridique : les entreprises sont contraintes de s'en remettre à des estimations probabilistes qui ne suffisent pas pour les mettre à l'abri d'éventuelles sanctions, ni pour pallier aux incertitudes juridiques par des mesures techniques qui si elles réduisent objectivement les risques de captation des données personnelles, ne suffisent pas non plus à régler la question de droit.

L'unique solution qui assure réellement une conformité stricte au droit européen résiderait donc dans la relocalisation complète des données et des traitements sur le seul territoire de l'EEE, entre les mains de prestataires européens échappant aux législations étrangères, soit la constitution d'un « cloud » véritablement souverain.

Si cette perspective est la seule à même de garantir la conformité réglementaire, elle apparaît très en décalage avec la réalité du marché actuel, qui repose sur des flux internationaux permanents et sur le recours généralisé à des champions du numérique qui sont - à ce jour du moins – bien plus souvent américains qu'européens. Les sous-traitants répartis dans le monde sont souvent localisés dans des pays qui se caractérisent à la fois par une main d'œuvre peu onéreuse et par des législations peu protectrices des libertés fondamentales, ceci expliquant souvent cela.

Au-delà de l'inextricable situation juridique dans laquelle sont plongées les entreprises européennes, il est donc aussi question de choix de société, et de la stratégie à adopter pour favoriser les entreprises européennes.

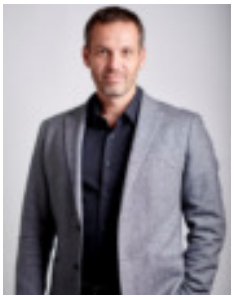
C'est une nouvelle illustration du fait que le RGPD, comme d'autres réglementations modernes liées à la « compliance », adressent des sujets aussi divers que l'efficacité économique, la sécurité technique, la lutte contre la cybercriminalité, mais aussi l'éthique, la protection des libertés fondamentales et les impératifs démocratiques.

Thomas Beaugrand,
Counsel
beaugrand@dsavocats.com
01.53.67.51.36

Pour plus d'information, notre équipe se tient mobilisée pour répondre à vos questions :

Catherine Verneret,
Associée
verneret@dsavocats.com
01.53.67.67.93

Antoine Gravereaux,
Associé
gravereaux@dsavocats.com
01.53.67.50.47



Sylvain Staub,
Associé
staub@dsavocats.com
01.53.67.50.23

Bertrand Potot
Associé
potot@dsavocats.com
01.53.67.61.09

A propos de DS Avocats

Fondé en
1972

350
professionnels du droit

24
bureaux

14
pays

4
continents

Un grand cabinet français de droit privé et public des affaires,

Créé en 1972 à Paris, DS Avocats a développé son savoir-faire au bénéfice des entreprises et des collectivités publiques. Cette double culture du public et du privé est un atout et constitue la signature du Cabinet.

organisé autour de spécialistes renommés dans tous les domaines du droit

Le Cabinet compte aujourd'hui près de 300 professionnels intervenant dans tous les domaines du droit des affaires, aussi bien en conseil qu'en contentieux. Nos équipes sont régulièrement citées parmi les meilleures du marché par les classements de référence dans le domaine juridique.

qui unissent leurs forces pour proposer une offre juridique de qualité et de proximité.

Les professionnels de DS Avocats interviennent en équipe (le cas échéant avec des partenaires non juridiques) pour permettre aux projets de ses clients d'allier excellence technique, expertise sectorielle et vision transversale.

Un des leaders européens en Asie,

DS Avocats, présent depuis plus de 30 ans en Chine, dispose aujourd'hui de 4 bureaux sur le continent asiatique.

résolument tourné vers l'international

DS Avocats poursuit et développe sa stratégie vers l'international, avec aujourd'hui 24 bureaux répartis dans 14 pays sur 4 continents.

www.dsavocats.com