BRADLEY JOSLOVE

Flux transatlantique de données : Des progrès mais...

Comme tous ceux qui effectuent des transferts de données personnelles vers les Etats-Unis, ou qui les conseillent, Bradley Joslove, avocat aux barreaux de Paris et de Washington, D.C., se félicite de l'accord entre Joe Biden et Ursula von der Leyen, en vue d'une décision d'adéquation de la Commission européenne visant à régulariser les transferts de données personnelles de l'Union européenne vers les Etats-Unis, probablement d'ici l'été prochain. Selon lui, les Américains ont consenti de réels efforts pour que le futur Privacy Framework soit conforme au RGPD et ne soit pas invalidé par la Cour de justice de l'Union européenne, en cas de recours plus que probable de Max Schrems. Avec son regard franco-américain qui met en lumière nos différences culturelles et d'attitude face à ces questions, il décrypte pour nous ce nouveau cadre, dont il espère qu'il sera approuvé par les instances européennes. L'avenir nous le dira.

Sylvie Rozenfeld : Le 13 décembre dernier, la Commission européenne a annoncé qu'elle avait officiellement entamé le processus d'approbation du cadre transatlantique de protection des données personnelles. En mars dernier, Joe Biden avait obtenu d'Ursula Von der Leyen un accord de principe sur la résolution de ce conflit juridique qui dure depuis 2013, date des révélations d'Edward Snowden sur les programmes de surveillance massives des étrangers. En octobre, le président des États-Unis a signé un executive order (décret exécutif), après plusieurs mois de concertation avec la Commission européenne. Reste désormais à attendre l'avis consultatif du CEPD, la position du Parlement européen et des États membres. La publication de la décision de la Commission est attendue pour le printemps prochain.
Bradley Joslove, vous êtes avocat aux barreaux de Paris et de Washington, D.C., associé au cabinet Bersay. Vous qui conseillez des sociétés françaises et américaines, est-ce que vous vous félicitez de la conclusion de cet accord ?

Bradley Joslove : Cet accord est fondamental. Encore faut-il que la décision d'adéquation soit adoptée. Depuis l'invalidation de la décision d'adéquation de la Commission européenne par la Cour de justice de l'Union européenne le 16 juillet 2020, toutes les entreprises européennes et américaines qui effectuent des transferts de données vers les États-Unis sont dans une situation extrêmement inconfortable, car elles doivent trouver une base légale autre que le Privacy Shield pour légitimer de tels transferts, et doivent en outre démontrer que les données à caractère personnel transférées bénéficieront d'un niveau de protection équivalent à celui prévu par l'Union européenne. Si tel n'est pas le cas, et c'est d'ailleurs l'argumentaire adopté par la décision de la Cour de justice de l'Union européenne, les parties au transfert doivent mettre en place des mesures de protection supplémentaires pour pallier cette absence d'adéquation du niveau de protection. Cette décision génère un vrai problème économique pour les PME qui veulent transférer des données personnelles aux États-Unis. Pour démontrer ce degré de protection, il faut faire une étude très détaillée du système juridique américain, y compris en ce qui concerne la capacité des services de renseignements américains à accéder aux données. Cette étude est complexe et onéreuse, d'autant plus pour les petites entreprises qui proposent des services de cloud. Même si une entreprise effectue cette étude, elle n'a pas de certitude que ce soit suffisant car il s'agit d'une auto-certification. Cela génère ainsi des coûts importants et beaucoup d'incertitude juridique.

« C'est la première fois dans ma carrière que j'ai dû dire à mes clients que je ne garantissais pas la solution proposée. »

Cela a compliqué la tâche des entreprises mais les données ont néanmoins continué de circuler.
Pas toujours. Au-delà de ces démarches complexes, dans certains cas il est impossible de trouver une mesure supplémentaire de protection. Par exemple, un prestataire de cloud américain ne peut plus proposer à une société française un service qui requiert que le prestataire américain ait accès aux données en clair. Le Comité européen de la protection des données (CEDP) considère d'ailleurs qu'il n'y a pas de moyen d'empêcher les services de renseignement américains d'avoir accès à ces données. C'est la première fois dans ma carrière que j'ai dû dire à mes clients que je ne garantissais pas la solution proposée, tout en donnant les meilleurs arguments possibles, et de les conseiller d'essayer de ne pas attirer l'attention des autorités de contrôle. Quand j'en parle à mes collègues qui interviennent dans le même secteur, ils font le même constat.

Venons-en à la proposition de décision d'adéquation. Le document de 134 pages du projet de texte n'apporte pas de changements fondamentaux mais se situe dans la lignée du Safe Harbor invalidé en 2015 par la CJUE et du Privacy Shield invalidé par la même Cour en 2020. Les sociétés américaines pourront bénéficier du mécanisme d'adéquation en s'engageant à se conformer à un ensemble d'obligations en matière de protection des données sans toutefois être obligées de se conformer au RGPD. Par ailleurs, les lois ayant des dispositions extraterritoriales comme le FISA ou l'Executive Order 12333 qui autorisent les agences de renseignement de collecter et traiter massivement des données, y compris relatives à des résidents européens, continueront de s'appliquer. Max Schrems, à l'origine des derniers recours devant la CJUE, a dit : Comme le projet de décision est basé sur le fameux Executive Order, je ne vois pas comment il pourrait survivre à une contestation devant la Cour de justice. Il semble que la Commission européenne ne fait qu'émettre des décisions similaires

encore et encore - en violation flagrante de nos droits fondamentaux.

Pensez-vous que cet accord opère un vrai changement ou n'est-ce qu'un aménagement cosmétique ?

Pour moi, cela se situe quelque part entre les deux. Max Schrems et certains autres veulent que les services de renseignements américains arrêtent la surveillance de masse. Or, ce n'est tout simplement pas possible pour l'administration américaine pour des raisons de sécurité nationale. De nombreux citoyens américains sont d'ailleurs du même avis. À cet égard, il faut comprendre qu'il existe des différences culturelles importantes entre les États-Unis et l'Europe. Je suis d'origine américaine et je vis en France depuis plus de 30 ans. Je représente un mélange des deux cultures. Je suis des deux pays mais aussi entre les deux. En matière de données personnelles, j'ai constaté ces différences culturelles et d'attitude entre les Américains et les Européens. Chaque pays garantit un ensemble de droits fondamentaux qui sont globalement similaires. C'est quand ces droits fondamentaux entrent en conflit que nous percevons le mieux ces différences. Par exemple, les Américains sont très attachés à la liberté d'expression et de manière presque absolue. Quand il y a un arbitrage à faire entre la liberté d'expression et d'autres droits, en général c'est le premier qui prime. C'est moins le cas en France où l'on interdit par exemple l'apologie des crimes contre l'humanité ou la haine raciale. Ce sont des restrictions à la liberté d'expression qui seraient invalidées aux États-Unis compte tenu de cette croyance culturelle bien américaine en la primauté de cette liberté. Du côté européen, il me semble que le droit à la protection des données à caractère personnel est considéré comme un peu plus fondamental que certains autres droits, comme on l'a constaté notamment avec l'arrêt Google Spain de la CJUE en 2014 qui a créé le droit à l'oubli. D'ailleurs, cet arrêt a été renforcé le mois dernier par un nouveau jugement de la CJUE impliquant Google et le droit à l'oubli.

En faisant l'arbitrage entre le droit à la vie privée et la responsabilité de l'État de protéger ses citoyens contre des menaces terroristes, les Européens placent davantage le curseur du côté du droit à la vie privée que le feraient les Américains. Par contre, il me semble que Max Schrems va un peu trop loin quand il soutient que la collecte de masse de données par les services de renseignement américains ne pourrait en aucune hypothèse être acceptée par le CJUE et ce peu importe la panoplie de limitations et protections qui pourraient le tempérer. Je ne sais pas si les protections contenues dans le Cadre transatlantique de protection des données personnelles vont assez loin pour satisfaire les juges de la CJUE, mais je ne l'exclus pas.

Il existe aussi aux États-Unis un droit à la vie privée.

Oui c'est un droit constitutionnel consacré par la Cour suprême des États-Unis, mais c'est un droit réservé aux citoyens américains. C'est un problème important dans le litige actuel car ce droit ne protège pas les étrangers. Or, les collectes massives de données ne portent que sur les données des étrangers et de telles collectes sont mises en œuvre hors des frontières américaines.

Est-ce que vous diriez que le système de protection des données personnelles aux États-Unis est moins protecteur que le système européen ou est-ce différent ?

Les deux : le système est différent, et, pour les Américains, il est moins protecteur que celui qui existe en Europe. Avec le Privacy Shield ou le futur Privacy Framework, les Européens dont les données personnelles sont envoyées à des sociétés américaines vont bénéficier d'un niveau de protection supérieur à celui accordé aux Américains, globalement équivalent à celui dont ils auraient bénéficié en Europe.

« Il s'agit d'une nette amélioration par rapport à l'Ombudsman, mais ce qui constitue la plus grosse différence avec le système antérieur est la possibilité de faire appel des décisions du CLPO auprès de la Data Protection Review Court. »

Voyons maintenant le contenu. L'un des points faibles du Privacy Shield identifié par la CJUE portait sur le manque de recours effectif pour les citoyens européens. L'article 47 de la Charte des droits fondamentaux impose l'accès à un recours judiciaire. Dans le projet de décision, pour obtenir réparation en cas de collecte et d'utilisation de leurs données par les agences de renseignement américaines, les plaignants devront s'adresser aux autorités nationales de l'UE, qui s'adresseront par la suite au gouvernement américain. Un agent de protection des libertés civiles (Civil Liberties Protection Officer ou PLCO), dépendant de la direction du renseignement américain serait chargé de vérifier les plaintes relatives à la violation du nouveau décret. Un recours est prévu auprès de la Cour de révision de la protection

des données (Data Protection Review Court), rattachée à l'exécutif américain.
Cet agent exercerait donc au sein même du bureau du directeur du renseignement national. Quid de son indépendance ? N'est-ce pas une réplique un peu améliorée de l'Ombudsman, rejeté par la CJUE ? Quelles garanties d'indépendance de cette cour ? Peut-on considérer qu'il s'agit d'un recours judiciaire au sens de la charte ?
Je pense qu'il existe une différence significative entre l'Ombudsman et le nouveau système à deux niveaux. Au premier niveau, le Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO, l'agent de protection des libertés civiles auprès du bureau du directeur des services de renseignements nationaux), dépend effectivement des services de renseignement. S'il n'y avait pas d'autres protections et contrôles, je dirais que le système n'aurait pas été très différent du précédent. Cependant, le CLPO dispose de protections contre l'influence des services de renseignement : il ne peut pas être licencié, sauf pour des motifs graves et limités. Il prend des décisions contraignantes, ce qui n'était pas le cas précédemment et il peut ordonner la suppression des données illégalement collectées. Il faut comprendre que son unique fonction est de protéger les données personnelles. Il s'agit d'une nette amélioration par rapport à l'Ombudsman, mais ce qui constitue la plus grosse différence avec le système antérieur est la possibilité de faire appel des décisions du CLPO auprès de la Data Protection Review Court. Selon moi, il s'agit d'un vrai tribunal créé par le département de la Justice et qui n'a rien à voir avec les services de renseignement. De vrais juges y siègeront, qui doivent être avocats avec une expérience en protection des données personnelles et en lois de la sécurité nationale. En revanche, il n'y a pas de recours prévu devant une cour d'appel fédérale ou devant la Cour suprême des États-Unis, ce qui est dommage.

« Compte tenu de ce principe et de la jurisprudence de la Cour suprême des États-Unis concernant l'intérêt à agir, la mise en place d'un « vrai tribunal » au sein de la branche judiciaire, comme le demande Max Schrems, serait inefficace. »

Comment être au courant que nos données ont été collectées par les agences de renseignements ?
C'est aussi pour résoudre cette difficulté que ce tribunal a été établi au sein de l'administration. Pour agir devant un tribunal classique, le plaignant doit démontrer son intérêt à agir, ce qui nécessite de prouver un préjudice. Si vous ne pouvez pas prouver que vos données personnelles ont été collectées, vous ne pouvez pas démontrer un préjudice. Compte tenu de ce principe et de la jurisprudence de la Cour suprême des États-Unis concernant l'intérêt à agir, la mise en place d'un « *vrai tribunal* » au sein de la branche judiciaire, comme le demande Max Schrems, serait inefficace. Le nouveau dispositif facilite la possibilité pour quiconque de contester cette collecte sans avoir à prouver un intérêt à agir. Le système est indirect, comme en France avec l'accès indirect aux fichiers régaliens par l'intermédiaire de la Cnil. Je vais vous donner un exemple personnel. Ma femme est française, mes enfants ont la double nationalité et on voyage beaucoup aux États-Unis. Pendant plusieurs années, ma femme et mes enfants étaient l'objet de fouilles systématiques dans tous les aéroports américains, comme s'ils étaient des terroristes présumés. J'ai pensé que les services de renseignement devaient avoir mis ma famille dans une sorte de « *fichier S* », à l'issue de leurs activités de surveillance. Je n'avais pas de preuves directes mais les circonstances le laissaient supposer. J'ai écrit à une certaine agence américaine et je n'ai pas eu de réponse mais après cela, ma famille n'a plus jamais été fouillée.

Comment se déclenchera le recours ?
Les personnes qui auront un indice indirect qu'elles ont fait l'objet d'une surveillance saisiront l'autorité de contrôle, la Cnil en France, qui contactera le CLPO. Ce dernier effectuera une enquête dont le résultat sera communiqué à la Cnil, disant soit que l'enquête n'a pas identifié des violations, soit que le CLPO a ordonné que des mesures appropriées soient entreprises, sans donner de détail et sans admettre ou nier que la personne concernée a été l'objet d'une surveillance. La personne concernée a le droit de faire appel des décisions du CLPO auprès de la Data Protection Review Court que j'ai déjà mentionnée.

La CJUE a exigé que la surveillance américaine soit « *proportionnée* » au sens de l'article 52 de la Charte des droits fondamentaux (CFR). Le décret américain évoque une surveillance « *nécessaire* » et « *proportionnée* » Quelle est la définition américaine de ce qui est « *nécessaire* » et « *proportionné* » ?
C'est la pratique qui va nous le dire. À ma connaissance, il n'y a pas de jurisprudence aux États-Unis à ce sujet car ce ne sont pas des termes

consacrés en droit américain. Aux États-Unis, nous avons le concept de « *reasonableness* », (raisonnable). Les termes européens ont donc été repris. On verra avec l'usage comment ils seront interprétés.

Mais les décisions ne sont pas publiques.
Un certain nombre d'organismes contrôlent les agences de renseignement dont certaines existaient déjà avant le décret. En plus du CLPO, il existe le Privacy and Civil Liberties Oversight Board (PCLOB) et la Foreign Intelligence Surveillance Court (FISC), qui produisent des rapports pour le Congrès et le public. Il faut savoir que les révélations de Snowden ont aussi choqué les Américains et ils ont mis en place un certain nombre de contraintes à l'égard des services de renseignements. Au niveau de l'UE, la Commission européenne, comme le CEPD, dispose d'un droit de regard. Elle va d'ailleurs pouvoir revoir sa décision d'adéquation après un an.

« Le Cadre transatlantique représente un vrai effort pour rendre le système américain équivalent en ce qui concerne le traitement des données personnelles des Européens. »

Un certain nombre de limitations et de garanties concernant l'accès aux données par les autorités publiques américaines sont prévues, lesquelles ?
Ce que contient le Cadre transatlantique de protection des données personnelles ressemble aux principes qui figurent dans le RGPD : une certaine transparence, la minimisation de la collecte de données, la limitation de la durée de conservation des données, la base légale du traitement, etc. Deux listes ont été créées : l'une concernant des collectes de données reposant sur des objectifs d'intérêt national autorisées et une autre sur des objectifs qui ne sont pas autorisés. Aux États-Unis par exemple, la collecte de données par les services de renseignements pour l'espionnage industriel est interdite, ce qui ne semble pas être le cas en France.

Finalement, peut-on trouver une compatibilité juridique entre le RGPD et le Cloud Act ou le FISA ?
Je pense que oui. Mais attention : le Cloud Act et le Fisa Act sont différents. Le Cloud Act ne concerne pas l'accès à des données à caractère personnel par les services de renseignement américains mais par les instances de justice fédérales et/ou locales. D'ailleurs, il n'était pas mentionné dans l'arrêt Schrems II. Tôt ou tard, on va arriver à un consensus. Il y a plus de 7 000 milliards d'euros d'échanges économiques entre les États-Unis et l'Europe, ce qui nécessite énormément d'échanges de données et notamment des données personnelles. Il est inimaginable d'arrêter ces échanges, on est donc condamné à trouver une solution. Aujourd'hui, la décision d'adéquation est encore au stade de projet. Le CEPD doit rendre un avis qui n'est que consultatif. La vraie décision sera prise par le Comité des représentants des pays membres à la majorité qualifiée. Cette décision est attendue d'ici la fin de l'été 2023. Le Parlement n'a pas quant à lui un rôle direct.

Il est à peu près sûr que si la décision d'adéquation est approuvée, Max Schrems intentera un recours contre cet accord, qui finira devant la CJUE. Je pense que le Cadre transatlantique de protection des données personnelles représente un vrai effort pour rendre le système américain équivalent en ce qui concerne le traitement des données personnelles des Européens, mais ce sera in fine la CJUE qui aura le dernier mot.

Propos recueillis par
Sylvie ROZENFELD