Les conséquences de l'invalidation du Safe Harbor sur le transfert de données personnelles

« Nul n'est censé ignorer… la protection des données personnelles », élevée au rang de droit fondamental par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Les données personnelles font toutefois désormais l'objet d'un véritable marché. Certains opérateurs économiques -les courtiers en données (*data brokers*)- ont même érigé la collecte et le traitement des données personnelles en objet social.

Dès 1995, le droit de l'Union européenne a cherché à trouver un équilibre entre la nécessaire protection des individus lors du traitement de leurs données personnelles et la libre circulation de celles-ci. La directive 95/46/CE encadre les transferts entre les pays membres de l'espace économique européen qu'elle soumet au respect de plusieurs principes. En ce qui concerne les transferts avec les pays tiers, elle ne les autorise que si le pays ou l'entreprise destinataire assure un niveau de protection suffisant aux données transférées. Mais qu'entend-t-on par : « niveau de protection suffisant » ? Cette notion ne fait l'objet d'aucune définition textuelle. La CJUE considère qu'elle ne signifie pas que la protection assurée dans l'État tiers doive être identique à celle garantie dans l'Union européenne, mais substantiellement équivalente.

Selon la Commission européenne, seuls quelques pays dans le monde répondent à ces exigences. Les Etats-Unis, principal acteur économique, fait partie des grands absents de cette liste. Et pour cause : leur conception de la protection des données personnelles est très différente de la conception européenne. Par exemple, si, en Europe, le traitement des données personnelles est conditionné par une autorisation légale spécifique, l'autorisation du traitement est de principe aux Etats-Unis (seule une interdiction spécifique ou un dommage peuvent limiter les possibilités de transfert). De plus, le droit européen ne permet pas de limiter la protection des données personnelles par contrat, alors qu'aux Etats-Unis la liberté contractuelle est très vaste en la matière.

Malgré ces différences importantes, le département du commerce américain et la Commission européenne ont négocié un accord international : le Safe Harbor, entré en vigueur au début des années 2000. Suite au scandale PRISM qui a révélé la surveillance massive de la NSA concernant des citoyens du monde entier, la confiance dans cet accord a été ébranlée. La crise a atteint à son paroxysme avec la décision de la CJUE du 6 octobre 2015, dite « *Schrem* », qui a invalidé le Safe Harbor sur le fondement de ses nombreuses failles, telles le mécanisme de l'auto-certification des sociétés américaines et la clause autorisant les services de renseignement américains à collecter des données d'utilisateurs européens en cas de menace pour la sécurité nationale.

La réaffirmation du pouvoir des autorités nationales de protection

L'article 8§3 de la Charte des droits fondamentaux de l'Union européenne énonce que « le respect [des règles relatives à la protection des données à caractère personnel] est soumis au contrôle d'une autorité indépendante ». Ces autorités, qui ont été instaurées dans chaque Etat membre de l'Union européenne suite à la directive de 1995, ont vu leur rôle s'effacer dans le cadre des transferts vers les Etats-Unis par la mise en place du Safe Harbor. L'autorité irlandaise de protection des données avait même refusé de donner suite à l'action d'un citoyen se plaignant du transfert de ses données vers les Etats-Unis en s'appuyant sur la décision de la Commission du 26 juillet 2000, qui considère que ceux-ci respectent les principes du Safe Harbor. Mais, par son arrêt de 2015, la CJUE a réaffirmé le rôle des autorités nationales de protection des données personnelles et a placé le principe de souveraineté sur les données au cœur de la doctrine européenne.

En effet, elle consacre le droit pour toute personne, qui s'estimerait lésée dans ses droits fondamentaux du fait d'un transfert de ses données personnelles vers un pays tiers, de saisir une autorité nationale de protection des données. Cela se traduit par la compétence des autorités nationales de protection pour examiner ce type de plainte, même en présence d'une décision de protection adéquate de la Commission. Un autre point fondamental de la décision réside dans le fait que la CJUE a remis en cause la possibilité pour la Commission européenne de limiter les hypothèses dans lesquelles les autorités nationales de protection des données pourraient suspendre les flux de données vers une organisation adhérant au Safe Harbor. Enfin, la Cour rappelle qu'en cas de doutes sérieux de la part de l'autorité nationale sur le caractère adéquat de la protection constaté dans une décision de la Commission, un recours devant les juridictions nationales qui pourront, le cas échéant, interroger la CJUE à titre préjudiciel, doit être permis.

Désormais, et dans l'attente d'un nouvel accord, les autorités nationales ont donc la possibilité d'accepter ou non le transfert de données vers les Etats-Unis, par une étude au cas par cas. Si cette décision permet une meilleure protection des données des européens, elle risque tout de même de causer une hétérogénéité des transferts : en effet, les Etats ne consacrent pas chacun exactement les mêmes normes de protection, une certaine liberté dans la transposition leur ayant été laissée par la directive. Ainsi, par exemple, l'approche anglaise facilite la circulation transfrontière, nécessaire au développement de la coopération internationale et du commerce mondial, de données à caractère personnel vers des pays tiers, en réduisant les formalités préalables aux traitements, alors, qu'en France, le contrôle de la CNIL est important. L'Allemagne a, quant à elle, annoncé que tout transfert de données vers les Etats-Unis est en l'état actuel illégal tant que la législation américaine en la matière n'aura pas changé. Malgré ces différentes réactions, les autorités de protection des données européennes, dont la CNIL, se sont réunies à plusieurs reprises au sein du G29 afin d'adopter une approche commune sur la question.

L'impact économique de la décision de la CJUE et les solutions de transfert alternatives

L'une des premières interrogations concerne le sort des 5 478 entreprises américaines, dont les GAFA. Sont aussi

indirectement touchées la plupart des sociétés françaises ou européennes qui font pour la majorité appel à des solutions en « cloud computing » pour des applications de back office ou de gestion client acquises auprès d'acteurs opérant aux Etats-Unis. Même si elles sont pour l'heure difficilement quantifiables, les conséquences commerciales de l'invalidation du Safe Harbor devraient être lourdes. Pour en avoir une idée, il est possible de se référer à un rapport publié en 2013 par la *Cloud security alliance* après les révélations Snowden qui chiffrait à 56% le nombre d'entreprises non résidentes américaines désormais moins enclines à utiliser des fournisseurs de cloud basés aux Etats-Unis.

En attendant la signature d'un éventuel Safe Harbor 2, la Commission recommande aux entreprises d'utiliser d'autres instruments juridiques. Notamment, les clauses contractuelles types, mises en place par la Commission européenne, et les règles internes d'entreprises (*binding corporate rules*). Si le premier de ces mécanismes apporte une certaine sécurité au responsable de traitement, il est surtout adapté aux transferts ponctuels puisqu'il nécessite la signature d'un jeu de clause par transfert, ce qui est administrativement lourd à gérer. Dans le cadre de groupes de sociétés, il est donc plus judicieux de recourir aux BCR qui permettent un transfert moins contraignant (tout en restant soumises à l'autorisation des autorités nationales de protection). C'est d'ailleurs cette politique qui a été adoptée par la société d'assurance AXA, anticipant l'invalidation du Safe Harbor. Même si la procédure a été simplifiée par la possibilité de désigner une autorité chef de file centralisant ainsi la procédure de validation, le temps estimé pour mettre ces règles en place reste long (AXA a mis 2 ans).

Outre les difficultés que cause l'annulation du Safe Harbor dans l'organisation de l'activité des entreprises, la décision *Schrems* risque de nuire à de nombreux accords actuellement en cours de négociation entre l'Union européenne et les Etats-Unis. En effet, un accord relatif au transfert de données personnelles policières et judiciaires pénales était sur le point d'être conclu. Si les négociations semblent en bonne voie, le Sénat américain s'étant prononcé en faveur de l'adoption du Judicial Redress Act qui conditionne l'adoption de l'Umbrella Agreement, certains eurodéputés ont contesté la conformité de cet accord aux garanties européennes au début du mois de février. Pire, cette bombe dans le domaine des données personnelles risque de compromettre les négociations relatives à l'accord TAFTA, en cours depuis 2013 entre l'Union européenne et les Etats-Unis, qui vise à être l'un des accords de libre-échange et de libéralisation de l'investissement les plus importants jamais conclus.

Vers un Safe Harbor 2 ?

La Commission européenne a annoncé le 2 février 2016 qu'elle avait conclu un accord avec les Etats-Unis sur le transfert de données : l'US-EU Privacy Shield. Pour la première fois, les Américains fournissent à l'Europe des assurances écrites que l'accès des pouvoirs publics aux données personnelles des européens sera soumis à des limitations claires et à des mécanismes de contrôle. Tout citoyen considérant que ses données ont été mal utilisées pourra adresser une plainte directement aux sociétés adhérentes du nouvel accord. Les autorités de contrôle européennes auront aussi la possibilité de transmettre ces plaintes au Département du Commerce américain et à la Federal Trade Commission. En outre, un système de résolution alternatif des conflits gratuit sera proposé. Enfin, un nouveau médiateur dédié aux questions d'accès aux données par les agences de renseignement devrait être créé.

Le G29 a pris acte de la publication du projet de décision d'adéquation de la commission européenne et l'analysera lors de sa séance plénière des 12 et 13 avril 2016 avec la plus grande attention afin de déterminer dans quelle mesure il peut contribuer à restaurer la confiance dans les flux de données transatlantiques. Il a rappelé dans un communiqué de presse du 3 février 2016 que quatre garanties doivent être satisfaites pour que l'accord puisse être adopté : le traitement doit être fondé sur des règles claires, précises et accessibles, un juste équilibre doit être trouvé entre les finalités pour lesquelles les données sont collectées et le droit des individus ; un système indépendant doit être mis en place pour assurer de manière effective les contrôles nécessaires et des voies de recours effectives devant des juridictions indépendantes doivent être crées. De plus, dès 2014, le Conseil d'Etat avait émis des propositions sur les modifications à apporter à l'accord.

En réalité, si un accord doit être mis en place le plus rapidement possible pour combler le vide juridique créé par l'arrêt de la CJUE, les différences de protection entre les parties à la négociation sont telles qu'il faudrait que les Etats-Unis modifient tout leur droit sur les données personnelles pour qu'il y ait une véritable adéquation avec le droit de l'Union européenne. Ces différences risquent encore de se creuser avec l'adoption du nouveau Règlement Général sur la Protection des Données. Selon Olivier Haas, avocat d'affaires « personne n'imagine vraiment que les Américains vont cesser leurs activités. L'objectif des européens pour le Safe Harbor 2 est seulement de limiter et d'encadrer ces pratiques, et de créer des mécanismes de recours et de contestation en cas d'abus ». Au regard des enjeux, le lobbying des grandes entreprises américaines a repris de plus belle, mettant sous pression l'Union européenne pour qu'elle renonce à certaines de ses exigences. Espérons que l'accord qui devrait être entériné dans quelques mois arrive à concilier les différents fondamentaux.

Flore BRUNETTI

Anne-Sophie LENDUSZKO