Boris Barraud, « Transferts de données personnelles de l'Union européenne vers les États-Unis : le "Privacy Shield" succède au "Safe Harbor" », *Revue Européenne des Médias et du Numérique* 2016, n° 38, p. 17 s.

manuscrit de l'auteur

Le 2 février 2016, la Commission européenne et le Département américain du commerce ont annoncé la conclusion d'un accord concernant la mise en place d'un nouveau cadre juridique pour les exportations de données personnelles de l'Union européenne vers les États-Unis. Devant remplacer le « Safe Harbor » récemment censuré par la Cour de Justice de l'Union Européenne, cet accord, baptisé « Privacy Shield », suscite la controverse.

En Europe, tout responsable de traitement de données personnelles doit assurer la sécurité et la confidentialité de ces données vis-à-vis des tiers non-autorisés. En particulier, en vertu de la législation européenne, il ne peut procéder à un transfert d'informations à caractère personnel vers un État n'appartenant pas à l'Union européenne. Seuls font exception les pays qui disposent de règlementations nationales offrant une protection au moins équivalente à celle assurée par le droit européen. Une dizaine de pays, tels que la Suisse, le Canada ou Israël, ont ainsi été qualifiés de « pays adéquats ».

Les États-Unis d'Amérique, pour leur part, ne sont pas éligibles au rang de pays adéquat puisqu'ils n'offrent guère de législation fédérale satisfaisante en matière de protection des données personnelles. Dans le même temps, à l'heure de la globalisation et de l'internet, il est difficile — et même impossible — de poser le principe d'une interdiction des échanges d'informations avec le berceau des Google, Facebook et autres Twitter. C'est pourquoi, dès juillet 2000, la Commission européenne avait conclu avec le Département du commerce des États-Unis un programme d'autorégulation, purement déclaratif, incitant les entreprises et organisations y adhérant à assurer aux traitements d'informations provenant d'Europe une protection équivalente à celle accordée dans l'Union européenne. Il s'agissait du « Safe Harbor », littéralement « sphère de sécurité ».

Mais, en 2000, le volume des échanges de données et le niveau de numérisation de la société et des individus étaient incomparables à ce qu'ils sont devenus avec l'avènement du Big Data et des réseaux sociaux. De plus en plus controversé, le « Safe Harbor » a été mis à mal, notamment, par les révélations d'Edward Snowden, en 2013, concernant le programme de surveillance de masse « Prism » de la NSA, auquel de grandes sociétés américaines ont collaboré. Surtout, Maximilian Schrems, un étudiant autrichien, a déposé différentes plaintes à l'encontre de Facebook, estimant que ses données stockées aux États-Unis n'étaient guère protégées. L'une d'elles a abouti à la remise en cause du « Safe Harbor » devant la Cour de Justice de l'Union Européenne (CJUE).

Un nouvel accord, ayant reçu le nom très marketing de « EU-US Privacy Shield » (« bouclier de la vie privée »), doit remplacer ce « Safe Harbor » devenu caduc et légaliser à nouveau les transferts à des fins commerciales de données personnelles de l'Union européenne vers les États-Unis.

Le « Privacy Shield », un accord rendu nécessaire par l'invalidation du « Safe Harbor »

Le 6 octobre 2015, la CJUE a invalidé l'accord « Safe Harbor ». Les juges européens, rappelant les révélations d'Edward Snowden, ont souligné combien était contradictoire l'attitude des entreprises américaines acceptant les conditions du « Safe Harbor » tout en donnant à la NSA accès aux données en leur possession dans le cadre du programme « Prism ». Et de considérer que « n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données ».

À compter de l'arrêt de la CJUE, tous les transferts de données personnelles de l'Europe vers les États-Unis sont devenus illégaux. Les entreprises peuvent bien s'appuyer sur des mécanismes juridiques alternatifs tels que les clauses contractuelles types recommandées par la Commission européenne ou les règles internes, mais l'illégalité de la plupart fait peu de doute à l'aune de la décision de la justice européenne. Les conséquences sont colossales puisque, quotidiennement, ce sont des milliards d'informations que Google et autres Facebook rapatrient aux États-Unis. La situation est alors devenue très curieuse puisque les autorités de protection des données personnelles des pays membres de l'Union européenne, regroupées au sein d'un groupe de travail appelé « G29 », ont décidé de faire preuve de pragmatisme : elles ont tout à la fois reconnu la parfaite illégalité de la plupart des transferts de données personnelles de l'Europe vers les États-Unis et décidé de ne pas intervenir afin de ne pas accentuer l'insécurité juridique née de l'invalidation du « Safe Harbor », l'économie numérique, en plein essor, étant aujourd'hui l'un des piliers de l'économie mondiale.

Après de nombreux mois de négociations intenses — elles avaient débuté bien avant l'annulation du « Safe Harbor » par la CJUE —, c'est finalement le 2 février 2016 que la Commission européenne et le Département américain du commerce ont rendu publique la conclusion d'un « accord de principe » devant servir de base à un nouveau cadre juridique pour les exportations de données personnelles entre les deux continents.

Les progrès du « Privacy Shield » par rapport au « Safe Harbor »

Baptisé « Privacy Shield », cet accord permet aux entreprises qui souhaitent transférer facilement des données vers les États-Unis de présumer que le régime juridique auquel elles obéissent offre aux données et à leurs titulaires une protection équivalente à celle dont bénéficient les européens en Europe. Seulement, pour ne pas risquer de se retrouver lui-aussi censuré par la CJUE, ledit accord devrait comporter de sensibles changements par rapport à l'insuffisant « Safe Harbor » de 2000. Or il est très incertain que les négociateurs soient parvenus à un résultat suffisant.

Le nouveau « bouclier » prévoit que les entreprises américaines collectant les données de citoyens européens devront respecter des obligations rigoureuses concernant le traitement de ces données et le respect des droits des personnes concernées. Différentes voies de recours, tant en Europe qu'aux États-Unis, sont consacrées. La Federal Trade Commission (FTC) pourra sanctionner et même exclure pour pratiques commerciales déloyales et trompeuses les entreprises participant au « Privacy Shield » qui n'en respecteraient pas les dispositions. Sous l'empire du « Safe Harbor », la FTC pouvait tout au plus demander à une société fautive de ne pas récidiver et les victimes ne pouvaient pas obtenir réparation pour la violation de leurs droits. De plus, l'accord prévoit la création d'un poste de médiateur (« ombudsman ») chargé de traiter les dossiers les plus sensibles. Et il comporte une innovante clause de révision annuelle censée permettre de suivre son application et, éventuellement, de l'adapter.

Si est en principe interdite la surveillance générale et inconditionnée des données personnelles des citoyens européens pratiquée par les services de renseignement américains, reste que de nombreuses incertitudes entourent ce « Privacy Shield », en premier lieu car il repose sur un engagement écrit du gouvernement américain à limiter la surveillance de masse à ce qui est « nécessaire et proportionné ». Or les notions de « nécessité » et de « proportionnalité » ne se présentent pas nécessairement sous le même jour en Europe et aux États-Unis. Elles nécessitent d'être interprétées et cette interprétation peut être très extensive.

De fortes critiques émises à l'encontre du « Privacy Shield »

Les GAFA et autres industriels et commerçants de l'internet se félicitent de l'accord trouvé et demandent son application la plus rapide possible. Mais, pour beaucoup d'observateurs, le « Privacy Shield » serait un « Safe Harbor 1.1 » bien davantage qu'un « Safe Harbor 2.0 », c'est-à-dire qu'il y aurait entre l'ancien et le nouvel accords un changement de version mineur et non majeur. Sur le fond, le « Privacy Shield » repose en effet sur le même raisonnement juridique que le « Safe Harbor » : les États-Unis n'ont pas à modifier leurs lois fédérales et les sociétés

privées s'engagent individuellement à fournir une protection « adéquate » aux données transférées depuis l'Europe. Il s'agit d'un programme d'autorégulation et déclaratif à l'identique du « Safe Harbor ».

Si la Commission européenne présente le « Privacy Shield » telle une « avancée majeure » et considère qu'il serait « radicalement différent » de l'ancien accord, lequel ne comportait aucune disposition relative aux pratiques du renseignement américain, et si la secrétaire au commerce des États-Unis, Penny Pritzker, s'est félicitée de la mise en place de ce qu'elle qualifie d' « accord historique [qui] va aider à la croissance de l'économie numérique en garantissant que des milliers d'entreprises européennes et américaines, et des millions de particuliers, continuent à avoir accès aux services en ligne », de nombreuses voix s'élèvent donc pour dénoncer ce qui serait un accord purement politique très insuffisant du point de vue de la sauvegarde des droits et libertés fondamentaux des européens, en premier lieu en ce qu'il n'exige aucune modification de la loi des États-Unis.

Du manque général de clarté du texte aux imprécisions quant aux notions clés et aux incertitudes quant à l'efficacité et à l'indépendance du médiateur, en passant par les incompatibilités entre certains principes américains et leurs équivalents européens ou par l'excessive complexité des voies de recours ouvertes aux citoyens européens, les opposants au « Privacy Shield » semblent ne pas manquer d'arguments. Selon eux, le changement de nom serait le seul véritable changement ; on aurait modifié la façade mais guère l'intérieur et les fondations du « Privacy Shield » seraient exactement les mêmes que celles du « Safe Harbor ». Pour beaucoup, le « Privacy Shield », en l'état, devrait inéluctablement se voir à son tour censurer par la CJUE.

Le G29, de son côté, a rendu un avis concernant le « Privacy Shield » le 13 avril 2016. Les autorités de protection des données personnelles y relèvent différents « sujets d'inquiétude » et signalent un « besoin urgent de clarifications » sur différents points clés tels que les pouvoirs et l'indépendance de l' « ombudsman » ou la mise en œuvre concrète des recours offerts aux citoyens européens en cas de violation de leurs droits sur le territoire américain. L'absence de « feu vert » de la part du G29 jette un flou sur l'avenir de l'accord, qui devrait être définitivement adopté par la Commission européenne avant la fin de l'année.

En définitive, c'est très logiquement et classiquement que le « Privacy Shield » est soutenu par la plupart des entreprises américaines et européennes du secteur du numérique, qui aspirent à un environnement juridique stable et peu contraignant afin de développer leurs activités, et critiqué par les associations et militants défendant les droits et libertés fondamentaux des individus, notamment leur droit au respect de la vie privée.