

L'Oncle Sam vous surveille

■ En invalidant le système "Safe Harbor", la Cour de justice de l'UE a accordé une victoire en trompe-l'œil aux organisations de défense des libertés. Des arrangements entre Etats permettent encore aux USA de récolter les données personnelles des citoyens européens.

Ce mardi 6 octobre, la Cour de justice de l'Union européenne a invalidé l'accord "Safe Harbor" qui encadre les transferts de données de citoyens européens vers les USA. Le système, légitimé par la Commission européenne en 2001 et ayant fait l'objet de nombreuses critiques, de la part des organisations de défense des libertés et par le Parlement européen en 2014, a été considéré par les juges comme *"portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée"*.

Autocertification

Le "Safe Harbor" "garantit" que les données stockées dans le serveur étasunien sont protégées par des normes analogues à celles en vigueur dans l'UE, alors que ces mécanismes de protection n'existent pas dans le droit US. Ce sont les sociétés adhérentes qui s'engagent à établir des procédures respectant les standards euro-

péens. Ainsi, plus de quatre mille entreprises étasuniennes peuvent stocker les données de leurs utilisateurs européens dans des serveurs situés sur le sol américain. Cependant, l'adhésion aux principes du "Safe Harbor" procède simplement par une autocertification de la société adhérente, une déclaration censée fournir des garanties quand aux possibilités de contestation auprès d'autorités indépendantes. Mais la qualité d'indépendance de ces autorités est peu déniée. Le "Safe Harbor" laisse la personne concernée démunie. C'est à elle de vérifier la situation de conformité de l'organisme étasunien

qui traite des données, c'est à elle de trouver et saisir l'autorité indépendante de contrôle apte à étudier son cas. Si malgré tous ces obstacles, une personne ou une entreprise a la possibilité de pouvoir constater un manquement à la procédure et qu'elle a la capacité d'entamer des poursuites, l'administration étasunienne peut encore invoquer la notion de "secret d'Etat", afin d'empêcher toute action judiciaire.

Coup d'arrêt à l'espionnage étasunien ?

Max Schrems, juriste et militant autrichien du droit à la vie privée, dont la plainte est à l'origine de la décision de la Cour de justice européenne, s'est réjoui de l'ar-

rêt en affirmant qu'il s'agit d'*"un coup sérieux porté à la surveillance mondiale des Etats-Unis qui repose massivement sur des partenaires privés"*. Pour lui, cet arrêt montre clairement que *"les entreprises américaines ne peuvent pas contribuer à l'espionnage américain en violant les droits fondamentaux européens"*.

Cependant, la décision complique à peine l'accès direct de l'Agence nationale de la Sécurité (NSA) aux

données des citoyens européens stockées sur le territoire étasunien. Il est loin de résoudre le problème, car les transferts de données peuvent aussi être autorisés grâce à des clauses contractuelles ou de "règles de bonne conduite" internes aux entreprises. C'est déjà le cas pour Google ou Microsoft. On reste ainsi dans un processus d'autocertification, cette fois au cas par cas, permettant, dans les faits, de ne pas respecter les règles européennes. L'arrêt de la Cour de justice de l'UE ne peut empêcher des sociétés comme Google ou Facebook, de fonctionner comme avant, mais celles-ci, en cas de procédure judiciaire, ne pourront plus s'abriter derrière un accord général de type "Safe Harbor" pour invalider les poursuites.

Cependant, c'est toujours la personne concernée qui doit seule franchir le maquis des procédures et, même en cas de succès, l'administration américaine a toujours la possibilité de bloquer toute action judiciaire.

Des accords entre Etats

Mais, l'élément le plus important, relativisant la portée de l'arrêt, consiste dans le fait que la surveillance mondiale exercée par les agences américaines ne repose pas seulement sur la collaboration des entreprises privées étasuniennes, mais sur les accords que les autorités US ont imposés à leurs partenaires étatiques, notamment européens. Ces dernières années, l'UE et les USA ont signé un ensemble d'arrangements en matière de remise des données personnelles: informations PNR des passagers aériens, données financières dans le cadre de l'affaire Swift. Un projet de transfert général a été négocié en 2009. Il s'agissait de remettre aux autorités américaines, une série d'informations privées, telles le numéro de la carte de crédit, les détails des comptes bancaires, les investissements réalisés, les connexions Internet,

la race, les opinions politiques, les mœurs, la religion. A chaque fois, l'UE a transformé sa propre légalité, afin de permettre au droit étasunien de s'appliquer directement sur son territoire. Rappelons les douanes US ont, depuis le 5 mars 2003, accès aux systèmes de réservation des compagnies aériennes situées sur le territoire de l'Union. Plusieurs accords, en 2004, 2006 et 2007 entre les USA et les institutions européennes ont légitimé la saisie des données des passagers européens.

Système asymétrique

En novembre 2009, le Conseil des ministres de l'Intérieur de l'UE a avalisé un texte qui permet aux autorités américaines de se saisir, sur les serveurs de la société Swift placés sur le sol européen, des données personnelles financières des citoyens des pays membres de l'Union. L'affaire Swift avait éclaté lorsque, en 2006, la presse étasunienne avait révélé que cette société avait, depuis les attentats du 11 septembre 2001, transmis clandestinement, au Département du Trésor US, des dizaines de millions de données confidentielles concernant les opérations de ses clients. La saisie par les autorités américaines était rendue possible par la particularité

du système Swift.

En effet, toutes les données contenues par le serveur européen, installé à La Haye, étaient également placées sur un second serveur placé aux

Etats-Unis. Ce qui permettait aux douanes étasuniennes d'en prendre possession, le droit américain autorisant cette saisie. Malgré la violation flagrante du droit européen de protection des données personnelles, ce transfert n'a jamais été remis en cause.

Au contraire, l'UE et les USA ont signé plusieurs accords destinés à autoriser cette capture.

Celui de 2009, formellement plus conforme aux critères européens puisque les données ne quittent pas le sol de l'ancien continent, installe un système asymétrique de capture des données personnelles: les autorités américaines ayant accès aux données européennes, sans qu'il soit question d'une quelconque réciprocité. Swift est un exemple inaugurant les transformations qui pourraient suivre l'arrêt de la Cour de justice: imposer aux entreprises de maintenir les données des ressortissants européens sur le territoire de l'UE et donner aux autorités US un accès direct à celles-ci.

**La surveillance
mondiale exercée
par les agences
américaines
ne repose
pas seulement
sur la collaboration
des entreprises
privées
étasuniennes,
mais sur les accords
que les autorités US
ont imposés
à leurs partenaires
étatiques,
notamment
européens.**