Note numéro 14
octobre 2015

Note du CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

La Cour de Justice de l'Union Européenne et la protection des données

Le « Safe Harbor »

La décision n°2000/520CE du 26 juillet 2000 de la Commission, constatant que les Etats-Unis respectent la « Sphère de sécurité », est annulée par l'arrêt CJUE C-362/14 *Maximillian Schrems/ Data Protection Commissionner* du 6 octobre 2015. L'autorité irlandaise de contrôle est tenue d'examiner s'il faut suspendre le transfert des données des abonnés européens de Facebook vers les Etats-Unis, au motif que ce pays n'offre pas un niveau de protection adéquat des données personnelles. C'est tout le dispositif du « Safe Harbor » qui est remis en cause. Qu'est-ce que la « Safe Harbor » ? Pourquoi la CJUE a-t-elle été saisie ? Quelles sont les dispositions de l'arrêt et leurs conséquences ? Autant de questions auxquelles il convient de répondre pour mieux comprendre le « séisme » qui affecte l'échange transatlantique des données.

La « Sphère de sécurité » ou *Safe Harbor*

La directive européenne 1995/46/CE du Parlement européen et du Conseil, en date du 24 octobre 1995, a pour objet la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation des données. Elle impose un niveau élevé de protection des droits et libertés des personnes, équivalent dans tous les Etats membres, en particulier pour permettre la libre circulation de leurs données à l'intérieur de l'Espace économique européen (EEE). Tout en reconnaissant que les flux transfrontaliers sont nécessaires au développement du commerce international, elle interdit le transfert de données à caractère personnel vers un pays tiers, lorsque celui-ci n'offre pas un « niveau de protection adéquat ».

Dans ce contexte, la Commission a ouvert des négociations avec les autorités américaines aboutissant à une décision n°2000/520 CE du 26 juillet 2000 relative à « la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes (FAQ), publiés par le ministère du commerce des Etats-Unis ». Cette décision, adoptée malgré les réticences exprimées le 5 juillet 2000 par le Parlement européen, définit sept principes qui doivent présider aux transferts transatlantiques :

- L'information des personnes résidant dans l'Espace économique européen de l'utilisation de leurs données ;
- La possibilité de refuser que les données soient transférées à des tiers ;
- le transfert autorisé ne peut être destiné qu'à un tiers respectant le même standard de protection ;
- la sécurité des données contre leur divulgation, leur altération, leur suppression ou un mésusage doit être garantie ;
- la finalité de l'usage des données doit être respectée ;
- les personnes doivent bénéficier d'un droit d'accès à leurs données et de modification ;
- la conformité des modalités d'application des règles précitées doit être contrôlée. L'entreprise certifiée doit être à nouveau contrôlée tous les douze mois.

Dans la pratique, les entreprises américaines « s'auto-certifient ».

La décision (6° et annexe VII) ne s'applique qu'aux entreprises qui relèvent du contrôle de la *Federal Trade Commission* (FTC) ou du *Department of Transportation* (DOT), ce qui représente un volume de plus de quatre mille entreprises. Elle ne concerne pas le secteur financier ou bancaire (accord SWIFT). Elle ne s'applique pas non plus lorsque sont établies des règles internes de transfert de données (*Binding Corporate Rules* ou BCR) validées par les 28 régulateurs nationaux (à vrai dire un seul en vertu du principe de reconnaissance mutuelle), des « clauses contractuelles types » élaborées par la Commission européenne, ou lorsque le transfert répond aux conditions définies par l'article 69 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La saisine de la CJUE

La Cour a été saisie d'un contentieux examiné par la *High Court of Ireland*. Celle-ci a posé une question préjudicielle aux fins de savoir si la décision de la Commission pouvait empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat et, si nécessaire, de suspendre les transfert de données.

Suite à l'affaire « PRISM », Maximilian Schrems, citoyen autrichien, s'est plaint du transfert de ses données à partir de la filiale irlandaise de Facebook vers les serveurs de l'entreprise situés aux Etats-Unis. L'autorité irlandaise de protection des données (*Data Protection Commissioner*) n'a pas donné pas suite en s'appuyant sur la décision de la Commission n°2000/520 CE du 26 juillet 2000 qui considère que les Etats-Unis respectent les principes de la « Sphère de sécurité », alors même que la protection des données à caractère personnel n'est pas garantie selon les mêmes règles par le droit américain.

Le dispositif de l'arrêt

Selon l'avocat général Yves Bot[1], « l'existence d'une décision de la Commission constatant qu'un pays tiers assure un niveau de protection adéquat aux données à caractère personnel transférées ne saurait annihiler ni même réduire les pouvoirs dont disposent les autorités nationales de contrôle en vertu de la directive sur le traitement de données à caractère personnel[2] ». S'agissant des Etats-Unis, il ajoute que «l'accès dont disposent les services de renseignement américains aux données transférées est constitutif d'une ingérence dans le droit au respect de la vie privée ».

La CJUE fait siennes les conclusions de l'avocat général. Pour la juridiction, la Commission n'a pas constaté que le niveau de protection accordé par les Etats-Unis était équivalent à celui garanti au sein de l'Union en vertu de la directive lue à la lumière de la Charte. En particulier, les exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des Etats-Unis l'emportent sur le régime de la « sphère de sécurité », ce qui oblige les entreprises américaines d'en écarter les règles dans de telles hypothèses. La Cour observe que la réglementation n'est pas limitée au strict nécessaire dès lors qu'elle autorise de manière généralisée, sans différenciation, limitation ou exception, sans possibilité d'exercer des voies de recours, la conservation de toutes les données à caractère personnel de toutes les personnes qui sont transférées de l'Union vers les Etats-Unis. En conséquence, elle annule la décision du 26 juillet 2000 de la Commission constatant que les Etats-Unis respectent la « Sphère de sécurité ».

1 curia.europa.eu, conclusions de l'avocat général dans l'affaire C-362/14 Maximilan Schrems/Data Protection Commissioner.

2 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Les conséquences

Conséquence immédiate de l'arrêt, la *High Court of Ireland* indique à Helen Dixon, commissaire de la DPC, qu'elle a l'obligation d'examiner la plainte de Maximilian Schrems. Dans un communiqué du 16 octobre, le groupe de travail « Article G29[3] », réuni à Bruxelles, « demande aux Etats membres et aux institutions européennes d'engager au plus vite les discussions avec les autorités américaines afin de trouver des solutions politiques, juridiques et techniques permettant de transférer des données vers le territoire américain dans le respect des droit fondamentaux ». Le G29 donne un délai de trois mois. Passée la fin du mois de janvier, les CNIL pourraient « mettre en œuvre toutes les actions nécessaires, y compris des actions répressives coordonnées ».

Plus de 4000 entreprises américaines implantées en Europe sont concernées par ses conséquences. Tout en étant salué par les défenseurs des droits de l'internaute, il inquiète les milieux économiques, notamment les PME. Celles-ci ne disposent pas, en effet, de services juridiques suffisamment étoffés pour établir des clauses contractuelles type, des règles internes d'entreprises, ou d'obtenir des autorisations de la CNIL (art.69 de la loi du 6 janvier 1978) prévoyant, hors du « Safe harbor », le transfert de données.

L'arrêt « Maximilian Schrems » va sans doute avoir pour première conséquence une accélération des renégociations du « Safe harbor 2.0 » (dont la date butoir avait été fixée au 31 mai 2015) et d'imposer le maintien sur le territoire de l'UE des données personnelles des ressortissants européens. Il renforce le rôle des autorités de contrôle indépendantes, comme la CNIL, dont les compétences devraient être élargies par la future loi « République numérique » portée par Axelle Lemaire. Il doit incontestablement inspirer la finalisation du règlement européen relatif à la protection des données.

Mais l'arrêt de la CJUE pourrait avoir aussi un « effet domino ». Günther Oettinger, commissaire européen à l'économie et à la société numériques s'interroge: « L'Europe est-elle-même un « Safe Harbor » ? ». Hans-Olaf Henkel, membre du Parlement européen est plus direct : « Je ne pense pas que la France soit exactement un « safe haven » et j'attends que des ressortissants allemands s'adressent à la Cour pour être sûrs que l'on ne puisse plus envoyer des données en France »…C'est une mise en cause à peine voilée de la loi de programmation militaire du 18 décembre 2013 et de la loi relative au renseignement du 24 juillet 2015 qui, selon leurs détracteurs, instaureraient un « système de surveillance de masse ». Le Conseil constitutionnel, par ses décisions des 23 et 24 juillet 2015, ne leur a pas donné raison.

* * *

Quoi qu'il en soit, on notera que la démarche isolée d'un homme de 27 ans, s'engageant dans la brèche ouverte par les révélations d'Edward Snowden, remet en cause tout un dispositif engageant 29 Etats. Une démonstration supplémentaire de l'extraordinaire pouvoir asymétrique qu'ont les particuliers dans l'espace numérique.

3 Le Groupe de travail G29 rassemble les CNIL d'Europe. Il tire son appellation de l'article 29 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

Déréférencement : les suites de l'arrêt Google Spain

Le déréférencement sur Google ne doit pas être limité aux extensions européennes du moteur de recherche.

Le 13 mai 2014, La Cour de justice de l'Union européenne a donné raison à un citoyen espagnol qui se plaignait du maintien de données le concernant et faisant état d'un problème ancien résolu qui apparaissaient lorsque son nom était tapé sur le moteur de recherche de Google. Saisie par l'Agence espagnole de protection des données, elle a rendu l'arrêt communément appelé « Google Spain » [1]. En s'appuyant sur les articles 7 et 8 de la Charte des droits fondamentaux, la Cour a considéré que Google procédait à un traitement de données à caractère personnel et a reconnu un « droit à l'oubli » devant être matérialisé par un déréférencement opéré sur demande de l'intéressé. Cette opération n'a pas pour effet de supprimer les données mais de les rendre inaccessibles. Seules sont exclues celles qui ont un caractère historique ou qui peuvent concerner une personne publique.

Dès l'annonce de l'arrêt, Google a été sollicité par plusieurs dizaines de milliers d'internautes et a, bon gré mal gré, donné satisfaction à la majorité d'entre eux. Toutefois, elle n'a procédé au déréférencement que sur les extensions européennes du moteur de recherche (.fr, .eu, .sp, etc.) en laissant un libre accès pour les autres terminaisons géographiques ou sur google.com. En agissant ainsi, Google a contourné la décision de justice, chacun pouvant accéder à des données en modifiant sa requête.

Google soutenait que l'arrêt ne s'appliquait pas hors de l'Europe, sauf à reconnaître au juge une compétence extraterritoriale du juge.

Saisie par des internautes mécontents, la présidente de la CNIL a adressé une mise en demeure publique à la société Google Inc.[2], laquelle a formé un recours gracieux.

Le 21 septembre 2015, la présidente de la CNIL a rejeté ce recours, estimant notamment que les pratiques de Google privent d'effectivité le droit reconnu par la CJUE en « faisant varier les droits reconnus aux personnes en fonction de l'internaute qui interroge le moteur et non en fonction de la personne concernée ». Elle demande « le plein respect du droit européen par des acteurs non européens offrant leurs services en France ».

1) - CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. C. Agencia Espanola de Proteccion de Datos et Mario Costeja Gonzalez, Aff. C-131/12. Le TGI de Paris a fait application de la jurisprudence de la CJUE en enjoignant Google de déférencer des propos que la justice avait déclarés diffamatoires (TGI Paris, ordonnance de référé, 16 septembre 2014, MM. c/Google France).

2) - Décision n°2015-047 du 21 mai 2015.