Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 117/15
Luxembourg, le 6 octobre 2015

Presse et Information

Arrêt dans l'affaire C-362/14
Maximillian Schrems / Data Protection Commissioner

La Cour déclare invalide la décision de la Commission constatant que les États-Unis assurent un niveau de protection adéquat aux données à caractère personnel transférées

Alors que la Cour est seule compétente pour déclarer l'invalidité d'un acte de l'Union, les autorités nationales de contrôle, saisies d'une demande, peuvent, même en présence d'une décision de la Commission constatant qu'un pays tiers offre un niveau de protection adéquat des données personnelles, examiner si le transfert des données d'une personne vers ce pays respecte les exigences de la législation de l'Union relative à la protection de ces données ainsi que saisir les juridictions nationales, au même titre que la personne concernée, afin qu'elles procèdent à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision

La directive sur le traitement des données à caractère personnel[1] dispose que le transfert de telles données vers un pays tiers ne peut, en principe, avoir lieu que si le pays tiers en question assure un niveau de protection adéquat à ces données. Toujours selon la directive, la Commission peut constater qu'un pays tiers assure, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection adéquat. Enfin, la directive prévoit que chaque État membre désigne une ou plusieurs autorités publiques chargées de surveiller l'application, sur son territoire, des dispositions nationales adoptées sur le fondement de la directive (« autorités nationales de contrôle »).

M. Maximillian Schrems, un citoyen autrichien, utilise Facebook depuis 2008. Comme pour les autres abonnés résidant dans l'Union, les données fournies par M. Schrems à Facebook sont transférées, en tout ou partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis, où elles font l'objet d'un traitement. M. Schrems a déposé une plainte auprès de l'autorité irlandaise de contrôle, considérant qu'au vu des révélations faites en 2013 par M. Edward Snowden au sujet des activités des services de renseignement des États-Unis (en particulier la National Security Agency ou « NSA »), le droit et les pratiques des États-Unis n'offrent pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays. L'autorité irlandaise a rejeté la plainte, au motif notamment que, dans sa décision du 26 juillet 2000[2], la Commission a considéré que, dans le cadre du régime dit de la « sphère de sécurité »[3], les États-Unis assurent un niveau adéquat de protection aux données à caractère personnel transférées.

Saisie de l'affaire, la High Court of Ireland (Haute Cour de justice irlandaise) souhaite savoir si cette décision de la Commission a pour effet d'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, le cas échéant, de suspendre le transfert de données contesté.

[1] 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 (JO L 281, p. 31).
[2] Décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (JO 2000, L 215, p. 7).
[3] Le régime de la sphère de sécurité comprend une série de principes relatifs à la protection des données à caractère personnel auxquels les entreprises américaines peuvent souscrire volontairement.

Dans son arrêt de ce jour, la Cour estime que **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 Charte des droits fondamentaux de l'Union européenne et de la directive. La Cour souligne à cet égard le droit à la protection des données à caractère personnel garanti par la Charte ainsi que la mission dont sont investies les autorités nationales de contrôle en vertu de cette même Charte.

La Cour considère tout d'abord qu'aucune disposition de la directive n'empêche les autorités nationales de contrôler les transferts de données personnelles vers des pays tiers ayant fait l'objet d'une décision de la Commission. Ainsi, **même en présence d'une décision de la Commission, les autorités nationales de contrôle**, saisies d'une demande, **doivent pouvoir examiner en toute indépendance si le transfert des données d'une personne vers un pays tiers respecte les exigences posées par la directive**. Néanmoins, la Cour rappelle qu'elle est seule compétente pour constater l'invalidité d'un acte de l'Union, tel qu'une décision de la Commission. Par conséquent, lorsqu'une autorité nationale ou bien la personne ayant saisi l'autorité nationale estime qu'une décision de la Commission est invalide, cette autorité ou cette personne doit pouvoir saisir les juridictions nationales pour que, dans le cas où elles douteraient elles aussi de la validité de la décision de la Commission, elles puissent renvoyer l'affaire devant la Cour de justice. **C'est donc en dernier lieu à la Cour que revient la tâche de décider si une décision de la Commission est valide ou non.**

La Cour vérifie alors la validité de la décision de la Commission du 26 juillet 2000. À cet égard, la Cour rappelle que la Commission était tenue de constater que les États-Unis assurent effectivement, en raison de leur législation interne ou de leurs engagements internationaux, un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive lue à la lumière de la Charte. La Cour relève que la Commission n'a pas opéré un tel constat, mais qu'elle s'est bornée à examiner le régime de la sphère de sécurité.

Or, sans qu'il y ait besoin, pour la Cour, de vérifier si ce régime assure un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union, la Cour relève que celui-ci est uniquement applicable aux entreprises américaines qui y souscrivent, sans que les autorités publiques des États-Unis y soient elles-mêmes soumises. En outre, les exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États-Unis l'emportent sur le régime de la sphère de sécurité, si bien que les entreprises américaines sont tenues **d'écarter, sans limitation, les règles de protection prévues par ce régime, lorsqu'elles entrent en conflit avec de telles exigences**. Le régime américain de la sphère de sécurité rend ainsi possible des ingérences, par les autorités publiques américaines, dans les droits fondamentaux des personnes, la décision de la Commission ne faisant état ni de l'existence, aux États-Unis, de règles destinées à limiter ces éventuelles ingérences ni de l'existence d'une protection juridique efficace contre ces ingérences.

La Cour considère que cette analyse du régime est corroborée par deux communications de la Commission[4], d'où il ressort notamment que les autorités des États-Unis pouvaient accéder aux données à caractère personnel transférées à partir des États membres vers ce pays et traiter celles-ci d'une manière incompatible, notamment, avec les finalités de leur transfert et au-delà de ce qui était strictement nécessaire et proportionné à la protection de la sécurité nationale. De même, la Commission a constaté qu'il n'existait pas, pour les personnes concernées, de voies de droit administratives ou judiciaires permettant, notamment, d'accéder aux données les concernant et, le cas échéant, d'obtenir leur rectification ou leur suppression.

[4] Communication de la Commission au Parlement européen et au Conseil, intitulée « Rétablir la confiance dans les flux des données entre l'Union européenne et les États-Unis d'Amérique » (COM(2013) 846 final, 27 novembre 2013) et communication de la Commission au Parlement et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire (COM(2013) 847 final, 27 novembre 2013).

S’agissant du niveau de protection substantiellement équivalent avec les libertés et droits fondamentaux garanti au sein de l’Union, la Cour constate **que, en droit de l’Union, une réglementation n’est pas limitée au strict nécessaire, dès lors qu’elle autorise de manière généralisée la conservation de toutes les données à caractère personnel de toutes les personnes** dont les données sont transférées depuis l’Union vers les États-Unis **sans qu’aucune différenciation, limitation ou exception ne soient opérées** en fonction de l’objectif poursuivi et sans que des critères objectifs ne soient prévus en vue de délimiter l’accès des autorités publiques aux données et leur utilisation ultérieure. La Cour ajoute qu’une règlementation permettant aux autorités publiques d’accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant **atteinte au contenu essentiel du droit fondamental au respect de la vie privé**.

De même, la Cour relève qu’une règlementation ne prévoyant aucune possibilité pour le justiciable d’exercer des voies de droit afin d’avoir accès à des données à caractère personnel le concernant, ou d’obtenir la rectification ou la suppression de telles données, porte **atteinte au contenu essentiel du droit fondamental à une protection juridictionnelle effective**, une telle possibilité étant inhérente à l’existence d’un **État de droit**.

Enfin, la Cour constate que la décision de la Commission du 26 juillet 2000 prive les autorités nationales de contrôle de leurs pouvoirs, dans le cas où une personne remet en cause la compatibilité de la décision avec la protection de la vie privée et des libertés et droits fondamentaux des personnes. La Cour considère que **la Commission n’avait pas la compétence de restreindre ainsi les pouvoirs des autorités nationales de contrôle**.

Pour toutes ces raisons, la Cour déclare la décision de la Commission du 26 juillet 2000 **invalide**. **Cet arrêt a pour conséquence que l’autorité irlandaise de contrôle est tenue d’examiner la plainte de M. Schrems avec toute la diligence requise et qu’il lui appartient, au terme de son enquête, de décider s’il convient, en vertu de la directive, de suspendre le transfert des données des abonnés européens de Facebook vers les États-Unis au motif que ce pays n’offre pas un niveau de protection adéquat des données personnelles.**

RAPPEL: Le renvoi préjudiciel permet aux juridictions des États membres, dans le cadre d'un litige dont elles sont saisies, d'interroger la Cour sur l'interprétation du droit de l’Union ou sur la validité d'un acte de l’Union. La Cour ne tranche pas le litige national. Il appartient à la juridiction nationale de résoudre l'affaire conformément à la décision de la Cour. Cette décision lie, de la même manière, les autres juridictions nationales qui seraient saisies d’un problème similaire.

Contact presse: Gilles Despeux ☎ (+352) 4303 3205