PRES@JE.COM Droit, Economie, Justice

DÉCEMBRE 2015 - N°27

L'affaire Maximillian Schrempf devant la Cour de Justice de l'Union européenne

Vers la fin de l'hégémonie américaine sur les données personnelles en Europe ?

par Thomas Cassuto, *magistrat, docteur en droit*

Les révélations fracassantes d'Edouard Snowden sur les méthodes américaines de surveillance et d'espionnage sont à l'origine d'un recours d'une importance cruciale pour les Européens. L'usager d'un réseau social ignore généralement que ses données personnelles et ses confidences sur la toile sont transférées vers les Etats-Unis de manière massive et automatique. « L'affaire Schrempf » est l'occasion pour la Cour de Luxembourg de stopper les dérives et d'imposer une meilleure protection des données intimes - santé, mœurs, opinions, modes de consommation - des citoyens européens.

« Les transferts de données à caractère personnel constituent un volet important et nécessaire des relations transatlantiques. Ils font partie intégrante des échanges commerciaux transatlantiques, [...] qui supposent le transfert de grands volumes de données entre l'Union européenne et les États-Unis ». C'est par ce rappel de la communication de la Commission européenne du 27 novembre 2013 que l'Avocat général Yves Bot introduit ses conclusions dans l'affaire Maximillian Schrempf contre Data Protection Commissioner[1] (DPC).

Les faits à l'origine de la saisine de la Cour de Justice de l'Union européenne (CJUE) concernent une grande majorité des citoyens européens. M. Schrempf, citoyen autrichien, est un client Facebook. Son profil est enregistré auprès de Facebook Irlande, siège européen du réseau social mondial et filiale de Facebook USA. M. Schrempf, s'appuyant sur les révélations d'espionnage massif d'Édouard Snowden, demande au DPC irlandais (l'équivalent de la CNIL) de vérifier les conditions de transfert de ses données personnelles vers les USA. Cette autorité a estimé que la requête était futile, vexatoire, car dépourvue de fondement juridique. Elle a donc refusé d'instruire cette plainte.

M. Schrempf a alors saisi la High Court, qui interroge à son tour la CJUE d'une question préjudicielle sur la régularité du dispositif européen de protection des données, qui établit la reconnaissance d'une sphère de sécurité (Safe Harbore) aux USA.

Le 6 octobre 2015, la CJUE a jugé qu'une autorité nationale de contrôle de la protection des données est compétente pour examiner la demande d'un particulier concernant la protection de ses droits à l'égard de données transférées vers un Etat tiers, en l'occurrence les Etats-Unis, lorsqu'il est invoqué que le droit ou les pratiques en vigueur dans cet Etat n'assurent pas un degré de protection adéquat. La cour annule en outre la décision 2000/520/CE de la Commission.

1. - Le principe de la sphère de sécurité est-il conforme au droit de l'Union européenne ?

La protection des données est organisée par la directive 95/46/CE qui prévoit l'interdiction de principe de la transmission de données personnelles hors de l'Union européenne, sauf reconnaissance par la Commission européenne d'une sphère de sécurité dans l'État de transfert. En application de cette directive, la Commission européenne, par la décision 2000/520/CE du 26 juillet 2000, a décidé que les États-Unis présentent des garanties conformes à la notion de sphère de sécurité, autorisant le transfert des données personnelles de l'UE vers ce pays. Il s'agit d'une décision à portée générale fondée sur

un contrôle a priori.

Dans ce contexte, la Cour rappelle que la protection des données personnelles peut être limitée notamment dans un but de sécurité nationale, dès lors que cette ingérence répond aux trois critères de légalité, de légitimité et de proportionnalité. Cette question comporte donc des enjeux de souveraineté. Par ailleurs, l'effectivité de la protection doit s'analyser à la lumière de la révélation de programmes massifs de surveillance.

Par cette décision, la Cour critique la Commission européenne, qui s'oppose au recours de M. Schrempf pour avoir maintenu la décision 2000/520 malgré une défaillance systémique et une rupture de la confiance dans ce domaine. La Cour souligne que le contexte de la décision de 2000 ayant changé, un contrôle a posterio et une suspension de la reconnaissance du Safe Harbor s'imposaient. Faisant référence à l'arrêt Digital Rights Ireland, la Cour, qui rappelle qu'elle est seule compétente pour invalider les actes de la Commission, annule la décision de 2000 comme contraire aux Traités et à la Charte. Cet arrêt reprend l'argumentation de l'Avocat général Bot qui critiquait le fait que les données transférées aux USA sont exposées à des programmes massifs de surveillance et que les Européens ne disposent pas, dans ce pays, de recours pour faire garantir leurs droits sur la protection de leurs données.

Ces critiques concernent le traitement des données par un fournisseur de services tel que Facebook dont les usagers/clients font un usage massif et renoncent a priori à tout droit sur leurs données personnelles. En effet, ces données, transférées vers les États-Unis, sont exploitées et peuvent permettre le profilage des individus à leur insu à des fins plus larges que strictement commerciales. Le citoyen européen ne dispose pour sa part d'aucune voie de recours ou de contrôle du traitement de ces données personnelles.

La décision rendue est donc symboliquement forte pour la protection des données et pour l'affirmation du rôle du juge européen dans la défense des droits des citoyens européens vis-à-vis des entreprises mondialisées. Reste encore à évaluer les conséquences de cette décision.

2. - Quelles conséquences ?

L'annulation de la décision 2000/520 n'implique pas un arrêt immédiat du transfert automatique ou systématique des données individuelles collectées sur le territoire d'une filiale vers sa maison mère aux États-Unis. Ainsi, toutes les applications téléphoniques informatiques etc. ne devraient pas cesser de fonctionner en ce qu'elles engendrent automatiquement le transfert de ces données y compris pour des données collectées dans un cadre par exemple médical, et ce, même avec le consentement de la personne.

D'autant plus que cette décision semble avoir été anticipée par les fournisseurs de services et les éditeurs d'applications pour obtenir le consentement au transfert des données par les usagers/clients. Il s'agit en effet pour ces sociétés de protéger le modèle économique reposant sur le transfert de données indispensable aux activités commerciales qui y sont adossées. L'arrêt Google contre l'Espagne du 14 mai 2014[2] illustre la capacité des grandes entreprises à s'adapter à une évolution soudaine du cadre juridique. Pour satisfaire à une telle décision, le traitement des données pourrait rester géographiquement localisé sur le territoire de l'UE au moyen d'adaptations plus techniques que juridiques. Cette solution pourrait susciter des critiques notamment de la part des entreprises qui ont toujours vu d'un mauvais œil les mécanismes tendant à cloisonner le droit applicable par référence à la localisation du client plutôt que celle du fournisseur. La restructuration de l'implantation opérationnelle de ces entreprises pourrait également avoir des conséquences fiscales.

Mais cette décision ouvre la voie à un contrôle renforcé du transfert des données par les autorités européennes indépendantes de contrôle telles que la CNIL. Forte de la légitimité d'une prééminence du droit communautaire fortement rappelée, outre les garanties particulières nationales en matière de protection des données personnelles, ces autorités pourraient exercer un contrôle très pointu sur la gestion des données personnelles par ces entreprises. Ce contrôle pourrait concerner le contenu des

contrats de prestation de service liés aux applications, les conditions de recueil du consentement des clients/consommateurs et la garantie que ces données ne sont pas transmises aux États-Unis.

Dans cette perspective, les industriels et les professionnels du droit ont commencé à déployer des solutions, qu'ils soumettront pour validation aux autorités nationales, destinées à satisfaire aux exigences imposées par la Cour, au droit communautaire issu de la directive de 1995 et, bien sûr, à préserver leur modèle économique.

Cette affaire, et en particulier ses orientations, ont suscité une vive inquiétude outre-Atlantique. La solution dégagée n'est pas une surprise. Les autorités américaines et les entreprises accoutumées à la jurisprudence de la Cour Suprême ne sous-estiment pas la capacité de la Cour de Luxembourg à bousculer l'ordre juridique communautaire établi et, par voie de conséquence, les relations juridiques entre les États-Unis et l'UE. Les autorités américaines ont indiqué qu'elles continueraient à administrer le « Safe Harbor » non par défi, mais comme gage de bonne foi. A brève échéance, il n'est pas certain que la décision 2000/520/CE, fruit de longues négociations politiques, puisse être utilement remplacée. Il est alors possible d'espérer que cette décision conduise le législateur américain à ouvrir l'accès aux voies de recours à des non-résidents et à des non-citoyens américains.

Le cadre juridique de la protection des données personnelles se développe à grande vitesse. Ainsi, parallèlement à la remise en cause du principe du Safe Harbor, l'Union européenne a conclu le 8 septembre 2015, au terme de quatre années de négociation avec les Etats-Unis, un accord-cadre sur la transfert de données dit « Umbrella Agreement ». Pour entrer en vigueur, cet accord devra encore être ratifié par l'ensemble des Etats membres et par le Congrès américain. En outre, la mise en œuvre de ces principes et de ces instruments devra s'interpréter à la lumière des dispositions futures de la directive et du règlement européens, présentés par la Commission européenne en janvier 2012, toujours en cours de négociation entre le Parlement européen et le Conseil. De même, la création d'un PNR (Passenger Name Record) européen constituera un marqueur dans l'élaboration de fichiers européens alimentés par des entités privées et mis à disposition des autorités publiques.

Ce cadre juridique complexe induit des enjeux humains et économiques majeurs. La décision de la Cour dépasse dès lors la stricte protection des données personnelles.

3. - Une annulation qui porte au-delà de la protection des données

Comme y invitait l'Avocat général, la Cour donne une leçon à la Commission dans le domaine de la protection des données personnelles. Indirectement, la Cour critique la doctrine générale des États-Unis en matière de traitement et de protection des données personnelles dont la réalité et l'ampleur ont pris une autre dimension avec les révélations d'Edouard Snowden.

Il faut souligner que le juge européen et en l'occurrence la High Court d'Irlande, en soumettant cette question préjudicielle à la Cour de Luxembourg, aura ouvert la voie à un rétablissement des équilibres. On comprend que ce n'est pas la surveillance en tant que telle qui est visée, mais son caractère massif, non discriminant, qui ne satisfait, de l'avis de la Cour, ni aux exigences de légalité, ni à celles de légitimité et de proportionnalité. En conséquence, les autorités fédérales américaines et les entreprises de l'internet pourraient être conduites à revoir en profondeur leur appréhension des données personnelles et à élaborer un droit plus respectueux des droits des citoyens sur leurs propres données. Encore faudra-t-il que le citoyen s'approprie utilement l'exercice de ces droits.

On pourra alors retenir que le juge européen aura fait preuve d'une audace et d'une efficacité exemplaires pour consacrer non seulement le principe fondamental de la protection des données personnelles consacré par le droit européen, mais également sa prééminence sur des activités économiques et de renseignement menées à l'étranger. On retiendra avec satisfaction que l'avenir du droit communautaire ne réside pas seulement dans l'harmonisation d'un droit cantonné au territoire européen mais également dans la défense de ses valeurs essentielles à l'étranger, ou à tout le moins dans la relation avec des États tiers. En tant que première puissance économique mondiale, l'UE peut en avoir les moyens politiques, à condition qu'elle en ait l'ambition judiciaire. Tenté par l'expression

d'une crise de légitimé, le citoyen pourrait trouver à s'y reconnaître.

Conclusion

La décision du 6 octobre 2015 ne peut être examinée en faisant abstraction des attentats du 11 janvier et du 13 novembre 2015. La propagande totalitaire est toujours liée à la confiscation, à la surexploitation et au détournement des moyens de communication. Le web et les réseaux sociaux ne peuvent plus se retrancher derrière un principe de neutralité qui protège ceux qui en abuse à des fins criminelles.

Il est possible, en modernisant effectivement les institutions judiciaires, de continuer à lutter efficacement comme le terrorisme, sans recourir à des moyens d'exception. Il appartient à l'État, et en particulier au juge, dans le respect de l'Etat de droit, de dégager et d'affermir des solutions qui permettent de préserver la souveraineté de la puissance publique garante de la sécurité des citoyens, dès lors que, derrière les écrans anonymes, se mènent des opérations destinées à tuer aveuglément et à tenter d'abattre la démocratie.

[1] Conclusions présentées le 23.09.2015 dans l'affaire C-362/14.

[2] V. (Dir. Thomas Cassuto) L'Europe du droit face aux entreprises planétaires, Bruylant septembre 2015, p. 111.

Télécharger le PDF de l'article

<< **Retour au sommaire**

PRES@JE.COM

Une publication de l'Institut PRESAJE
(Prospective, Recherche et Etudes Sociétales Appliquées à la Justice et à l'Economie)
30 rue Claude Lorrain 75016 Paris
Tél. 01 46 51 12 21 - E-mail : contact@presaje.com - www.presaje.com
Directeur de la publication : Michel Rouger

Pour ne plus recevoir d'e-mails de la part de Presaje, cliquez ici **>> CONSULTER LES PRECEDENTS NUMEROS**