Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10
Email : ccbe@ccbe.eu – www.ccbe.eu

Commentaires du CCBE concernant la réévaluation de l'accord *Privacy Shield* UE-États-**Unis**

25/09/2017

Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays, soit plus d'un million d'avocats européens.

Avant la première réévaluation annuelle du bouclier de protection des données (*Privacy Shield*) en septembre 2017, le CCBE exhorte la Commission européenne à suspendre sa décision d'exécution 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis au motif que les États-Unis d'Amérique (États-Unis) n'assurent pas un niveau de protection des données à caractère personnel essentiellement équivalent à celui garanti par l'Union européenne (UE).

Contexte

Le 6 octobre 2015, la Cour de justice de l'Union européenne (CJUE) a rendu son jugement dans l'affaire *Schrems contre Data Protection Commissioner*, invalidant la décision 2000/520/CE relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité ».

En conséquence de ce jugement, le 2 février 2016, la Commission européenne et le gouvernement des États-Unis sont parvenus à un accord politique sur un nouveau cadre pour les échanges transatlantiques de données à caractère personnel à des fins commerciales : le bouclier de protection des données UE-États-Unis.

La Commission européenne a adopté, le 12 juillet 2016, une décision d'exécution relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, renforçant la nécessité de protection des données d'une manière de protection des données d'une manière substantiellement équivalente à celle assurée par le droit de l'Union européenne. A cet égard, la Commission a considéré la loi américaine du 4 novembre 2015 (*Judicial Redress Act*) qui étend, notamment aux ressortissants de l'Union européenne, les garanties bénéficiant aux citoyens et résidents américains en matière d'utilisation des données personnelles par les agences fédérales en application du *Privacy Act*, comme une avancée substantielle et une garantie importante.

On rappellera que le groupe de travail Article 29 sur la protection des données (G29), dans sa déclaration du 29 juillet 2016, avait cependant émis des réserves sur le bouclier de protection des données au regard de l'accès des autorités publiques américaines aux données transférées par l'Union européenne. Il relevait les problèmes liés au manque d'indépendance et de pouvoir du médiateur (*Ombudsperson*) ainsi qu'au manque de garantie concrète propre à empêcher les services de renseignement américains d'effectuer la collecte massive et indiscriminée de données personnelles.

Dans les affaires jointes *Tele2 Sverige AB contre Post-och telestyrelsen* (C-203/15) et *Secretary of State for the Home Department contre Watson et autres* (C-698/15) du 21 décembre 2016, la CJUE a donné plus d'indications quant aux restrictions que la législation doit imposer dans l'accès aux données conservées afin de respecter la Charte des droits fondamentaux de l'UE.

Le bouclier de protection des données fait actuellement l'objet de deux recours d'associations devant le Tribunal de l'Union européenne.

Préoccupations du CCBE concernant la légitimité du bouclier de protection des données

Compte tenu des normes identifiées par la CJUE en vertu des libertés et droits fondamentaux garantis par le droit de l'UE, le CCBE considère que le bouclier de protection des données UE-États-Unis présente un certain nombre de lacunes importantes qui suscitent des préoccupations quant à sa légitimité, notamment en ce qui concerne l'absence de garanties contre les programmes de surveillance vastes et étendus des États-Unis.

À cet égard, les *Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance* (ci-après dénommées « Recommandations du CCBE »), adoptées le 28 avril 2016, énoncent des normes à sauvegarder afin de garantir que les principes essentiels du secret professionnel ne soient pas remis en cause par des pratiques de l'État consistant à intercepter les communications et à avoir accès aux données des avocats à des fins de surveillance ou de maintien de l'ordre. Voici un résumé des principales préoccupations du CCBE concernant le bouclier de protection des données, qui découlent directement de ces Recommandations.

Absence de contrôle législatif contraignant

Toutes les activités de surveillance doivent être réglementées de manière transparente et avec les précisions nécessaires afin d'éviter le risque de manquement arbitraire aux droits de l'homme[1]. À cet égard, le bouclier de protection des données ne fait référence qu'aux « lignes directrices et politiques du Département de la Justice » ou aux « politiques transparentes du Département de la Justice ». En tant que base juridique de règles claires, précises et accessibles, ces politiques et lignes directrices ne peuvent être considérées comme une forme de contrôle législatif contraignant. Par ailleurs, l'expression « sécurité nationale » dans le bouclier de protection des données n'est pas définie avec un degré de précision permettant de garantir que les infractions à la protection des données puissent être examinées efficacement par les tribunaux pour garantir le respect d'un critère strict de ce qui est nécessaire et proportionné.

Mécanismes de contrôle juridictionnel indépendants

Toute atteinte aux droits fondamentaux à la vie privée et à la protection des données devrait être contrôlée par un organe judiciaire inamovible et indépendant à la fois financièrement et politiquement du pouvoir exécutif, car seul un juge peut offrir les garanties nécessaires d'indépendance. Les Recommandations évoquent de nombreuses exigences[2] concernant la nature du contrôle et le mandat de l'organe de contrôle qui doivent être respectées par celui-ci avant que le contrôle des activités de surveillance puisse être jugé satisfaisant.

Premièrement, les Recommandations précisent que le contrôle doit être confié à un organe judiciaire inamovible et indépendant à la fois financièrement et politiquement du pouvoir exécutif[3]. Le cadre juridique du mécanisme de surveillance du bouclier de protection des données comporte plusieurs niveaux et se compose de deux grandes parties : le contrôle interne et le contrôle externe. Apparemment, aucun des organes de contrôle interne ne peut être financièrement et politiquement indépendant du pouvoir exécutif étant donné qu'ils en font fondamentalement partie, de sorte que le contrôle interne ne répondra pas à l'exigence de contrôle de la manière énoncée ci-dessus. Dans le cadre du bouclier de protection des données, la surveillance externe est assurée par ce qui est décrit comme des organes judiciaires[4], y compris les comités de renseignement du Congrès et le *Privacy and Civil Liberties Oversight Board*. Ces deux dernières instances ne sont pas des organes judiciaires, de sorte que l'exigence du contrôle ne peut être respectée que par la *United States Foreign Intelligence Surveillance Court.* Il convient toutefois de noter que la procédure devant cette juridiction est ex parte, ce qui signifie que les personnes concernées peuvent ne pas être entendues, voire même ne pas être au courant de l'affaire.

Il convient également de souligner que les caractéristiques d'une activité de surveillance donnée dépendent de la base juridique invoquée lors de la mise en œuvre des programmes de surveillance. Par exemple, les activités de surveillance menées en vertu de l'article 215 du *Foreign Intelligence Surveillance Act* sont presque entièrement soumises au contrôle judiciaire préalable de la *United States*

1 Recommandations du CCBE, points 2.1 à 2.4, pages 19-20.
2 Recommandations du CCBE, points 4.1 à 4.7, pages 22 à 25.
3 Recommandations du CCBE, points 4-2 et 4-3, page 22.
4 L'annexe VI du bouclier de protection des données invoque la section 702 du *Foreign Intelligence Surveillance Act*.

Foreign Intelligence Surveillance Court. En revanche, les activités de surveillance reposant sur le décret 12333 ne font l'objet d'aucun contrôle juridictionnel préalable ni ultérieur.

La loi doit accorder des pouvoirs contraignants, appropriés, et proportionnels à l'organe de contrôle pour qu'il s'acquitte de son rôle. Ces compétences doivent permettre à l'organisme de prendre des décisions exécutoires en tout état de cause[5]. Toutefois, le bouclier de protection des données précise uniquement la compétence plutôt limitée du médiateur et, même si l'on considère le médiateur comme un organe de contrôle (ce qui n'est pas précisé dans le bouclier de protection des données), il est évident que le médiateur ne dispose d'aucun pouvoir effectif puisqu'il ne peut que demander des mesures supplémentaires à l'organe approprié du gouvernement des États-Unis ou demander des renseignements à d'autres entités gouvernementales.

Il convient également de souligner que si l'organe de contrôle n'a pas à tout le moins le pouvoir de mettre fin à la surveillance illégale, il ne peut dès lors pas accomplir son mandat de manière satisfaisante. Un organe de contrôle ne peut prendre des décisions exécutoires que s'il est en mesure d'ordonner aux autorités de cesser et de mettre fin à des activités de surveillance illégale ou d'ordonner la destruction permanente d'informations obtenues par surveillance directe et indirecte.

Manque de voies de recours efficaces

Afin d'assurer une protection juridique efficace contre la surveillance illégale, il est nécessaire que des voies de recours soient ouvertes aux avocats et à leurs clients qui ont fait l'objet d'une surveillance illégale. Le gouvernement des États-Unis considère que les protections prévues par la Constitution des États-Unis, qui interdit les perquisitions et saisies « déraisonnables » et établit l'exigence d'un mandat pour empêcher de telles actions, ne s'appliquent pas aux personnes non ressortissantes des États-Unis se trouvant hors du territoire des États-Unis. Par conséquent, dans le contexte de la surveillance et du renseignement, les citoyens de l'UE qui ne sont pas ressortissants des États-Unis ne bénéficieront pas de ces protections constitutionnelles, alors que dans l'UE, n'importe quelle personne peut saisir la justice si elle a une raison légitime de soupçonner une ingérence dans ses droits fondamentaux, quelle que soit sa nationalité.

Bien que le bouclier de protection des données indique de manière générale que des voies de recours judiciaires et administratives sont à la disposition des personnes aux États-Unis d'Amérique, ceci totalement remis en cause par le décret *Executive Order 13768 Enhancing Public Safety in the Interior of the United States*.

En effet, ce décret prévoit expressément que les dispositions du *Privacy Act* ne s'appliqueront plus à ceux *« qui ne sont ni des citoyens des Etats-Unis ni des résidents permanents légaux »*. Les garanties et recours du *Privacy Act* ne bénéficieraient donc plus aux ressortissants de pays de l'Union européenne qui ne sont pas résidents permanents légaux aux États-Unis. En conséquence, ce décret semble prévaloir sur les garanties accordées dans le cadre des discussions sur le bouclier de protection des données.

Ce décret permet également à la NSA de partager avec 16 autres agences gouvernementales de grandes quantités de données personnelles de personnes non-américaines et ce, sans disposer de mandat, de décision de justice ou d'autorisation du Congrès.

Le Congrès a par ailleurs autorisé les fournisseurs d'accès internet à vendre les données personnelles de leurs abonnés, en ce compris l'historique et d'autres informations privées, sans leur consentement.

Un décret présidentiel ayant une force inférieure à celle d'une loi dans le système juridique américain, il a pu être allégué que le décret du 25 janvier 2017 ne devrait pas être considéré comme pouvant remettre en cause le *Judicial Redress Act* du 4 novembre 2015.

Toutefois, ce décret présidentiel, à tout le moins, (i) acte l'intention du pouvoir exécutif américain de revenir sur les garanties précédemment accordées aux ressortissants des pays de l'Union européenne s'agissant de la protection de leur données personnelles, (ii) laisse craindre qu'en pratique les autorités gouvernementales américaines qui dépendent directement du pouvoir exécutif cherchent à s'affranchir des engagements pris lors de la présidence Obama à l'égard de l'Union européenne et (iii) expose les citoyens européens à l'exploitation non autorisée de leurs données personnelles, sans recours effectif.

[5] Recommandations du CCBE, point 4.7, page 24.

Dans un communiqué du 15 février 2017, le G29 a indiqué adresser une lettre aux autorités américaines pour solliciter une clarification sur l'impact de ce décret sur le bouclier de protection des données. Si une réponse a pu éventuellement être apportée par les autorités américaines, celle-ci n'a pas été rendue publique.

Jan Philipp Albrecht, rapporteur du Parlement européen sur la protection des données, s'est alarmé de la situation et a déclaré : *« si cela est confirmé, la Commission européenne doit immédiatement suspendre le Privacy Shield et sanctionner les Etats-Unis d'avoir violé l'accord »*.

Réévaluation du bouclier de protection des données

Aux termes de l'article 4 du bouclier de protection des données, entré en vigueur le 1er août 2016, une réévaluation annuelle du dispositif est prévue.

Le paragraphe 5 de l'article 45 du règlement européen sur la protection des données personnelles (RGPD), prévoit la compétence de la Commission pour abroger, modifier ou suspendre la décision d'adéquation qu'elle a prise *« lorsque les informations disponibles révèlent, en particulier à l'issue de l'examen visé au paragraphe 3 du présent article, qu'un pays tiers (…) n'assure plus un niveau de protection adéquat au sens du paragraphe 2 de l'article 45 »*.

Le 12 juillet dernier, la Commissaire à la Justice, Věra Jourová, a prononcé un discours devant la délégation pour les relations avec les États-Unis du Parlement européen, concernant les modalités de réévaluation du bouclier de protection des données. Elle a encouragé le maintien du Bouclier de protection des données à condition que les garanties sur lesquelles il a été construit soient maintenues, et, notamment, le Médiateur en charge de gérer les plaintes des citoyens contre ingérences des autorités américaines ainsi que les garanties contenues dans le *Presidential Policy Directive 28*, mis en place par le Gouvernement Obama. La Commissaire n'a pas mentionné les effets de l'*Executive Order* du 25 janvier 2017 sur la protection des données personnelles des citoyens européens.

Dans le cadre de cette réévaluation annuelle, le CCBE invite la Commission à exercer ses pouvoirs en vertu du paragraphe 5 de l'article 45 du règlement européen sur la protection des données personnelles (RGPD) en vue de suspendre le bouclier de protection des données. Concernant les préoccupations exprimées plus haut quant à la légitimité du bouclier de protection des données, il apparaît, notamment à la suite du décret du 25 janvier 2017, que les Etats Unis n'assurent plus une protection adéquate des données personnelles des ressortissants des pays membres de l'Union européenne.

La renégociation de l'accord Privacy Shield devra reposer sur des garanties sérieuses de protection des données de la part des États Unis, spécialement s'agissant de l'accès des autorités publiques aux données personnelles et du processus de certification des entreprises américaines.