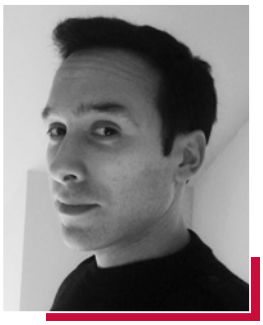

Nicolas OCHOA
Président de la Ligue pour la Protection des Données Personnelles (LPDP), Consultant, Docteur en droit qualifié aux fonctions de maître de conférences.

La spécificité de la protection des données personnelles en matière fiscale.

L'exemple de l'annulation probable du FATCA

Mots-clés : fiscalité - protection des données personnelles - CNIL - CEDH

La protection des données personnelles s'impose en matière fiscale mais avec des atténuations dues aux spécificités de cette matière régalienne. Toutefois, la complexité de la norme fiscale fait planer un risque juridique comme le montre la non-conformité probable de la convention d'échanges automatiques de données entre la France et les États-Unis à la jurisprudence de la Cour européenne des droits de l'Homme.

L'expression « protection des données personnelles » constitue souvent un raccourci impropre pour désigner l'ensemble des instruments juridiques encadrant l'activité de traitement de données personnelles. Si l'on prend la peine de se pencher sur l'économie de leurs dispositions, on se rend compte assez rapidement que ces textes sont structurés autour d'un objectif, libéraliser l'activité de traitement de données personnelles – autrement dit ficher les personnes –, et d'une limite, protéger les personnes concernées de l'abus de fichage. La seule raison d'être aujourd'hui de cette métonymie relève du marketing législatif : il n'est politiquement pas correct d'énoncer que la Loi informatique et libertés[1] vise à garantir l'opération juridique du fichage le plus étendu possible des personnes physiques[2]. Aussi, que recouvre réellement l'expression « protection des données personnelles » ? Un excellent résumé peut en être donné à l'article 8 de la Charte des droits fondamentaux de l'UE, qui énonce que :

« *1. Toute personne a droit à la protection des données à caractère personnel la concernant.*

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Il ne s'agit là que d'un résumé, les instruments encadrant les traitements de données personnelles comportant des dispositions plus nombreuses et plus précises, tels que le droit de s'opposer à un traitement, le droit à l'oubli ou le droit au recours administratif et juridictionnel contre un responsable de traitement etc.

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF 7 janvier 1978, p. 227.

[2] OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, thèse, Paris 1, 2014.

doi:10.3166/gfp.2017.00123

Les spécificités de la protection des données personnelles dans le contexte fiscal

Le sujet de cet article invite à s'interroger sur l'existence éventuelle d'une spécificité de ce premier objet dans un contexte fiscal, plus précisément dans un contexte de traitements de données personnelles par l'administration fiscale.

De prime abord, une telle spécificité ne saute pas aux yeux. En effet, le développement du numérique a encouragé, depuis déjà un certain nombre d'années, la multiplication des traitements de données personnelles tant à des fins privées que publiques. Dans la sphère publique, cela s'est traduit, notamment, par le développement de l'e-administration, impliquant de manière privilégiée une numérisation et parfois une automatisation des échanges de données entre administrations et administrés, et parfois entre administrations elles-mêmes. La raison d'un tel développement tient aux gains en termes d'efficience de l'action publique, qui devient plus rapide, plus efficace et en même temps plus proche de l'administré. L'administration fiscale n'est pas restée à l'écart de ce mouvement de fond, en témoignent le nombre important de traitements créés ces dernières années.

Pour autant, une telle évolution n'est pas sans risque pour les droits et libertés des personnes physiques concernées. En effet, si le développement de ces traitements publics de données personnelles a pour conséquence une amélioration notable de la qualité et de la réactivité de l'action publique, elle entraîne également un certain nombre de violations des droits et libertés des droits fondamentaux des administrés. Ces violations trouvent essentiellement leur origine dans une méconnaissance des standards posés par la CEDH et l'UE en matière de protection des données personnelles. En effet, si la loi « informatique et libertés » demeure encore sous son intitulé originel, l'essentiel du droit est, de longue date, affaire du droit européen. D'abord par l'action du Conseil de l'Europe d'élaboration de la première convention internationale d'encadrement des traitements de données personnelles (la convention n° 108), complétée et renforcée par l'interprétation par la CEDH de l'article 8 de la CESDH garantissant aux individus résidant dans les États parties le droit au respect de leur vie privée. Ensuite par l'adoption, au niveau des Communautés européennes puis de l'UE, de standards communs d'encadrement des traitements de données personnelles, comme la directive 95/46 du 24 octobre 1995[3] ou, plus proche de nous, le Règlement général relatif à la protection des données personnelles du 27 avril 2016[4].

Au delà de ce contexte global dans lequel l'administration fiscale s'inscrit, comme tout responsable public de traitement de données, trois spécificités peuvent être identifiées. Premièrement, l'activité de l'administration fiscale est, à l'instar de l'activité bancaire ou assurantielle, toute entière tournée vers le traitement de données personnelles.

Deuxièmement, les traitements de l'administration fiscale de cessent de se multiplier, tant dans l'ordre interne qu'à destination d'autres États. La raison de cette augmentation quantitative des traitements tient dans la volonté de rendre les services de l'administration fiscale plus efficients, notamment en vue de prévenir la fraude.

Enfin, la dernière spécificité de l'activité de traitement de données personnelles en matière fiscale tient au caractère régalien de ce secteur d'activités. Cela ne signifie pas que le droit des données personnelles ne s'applique pas, mais qu'il s'y applique de manière parfois atténuée. En témoignent plusieurs points textuels de rencontre entre droit fiscal et droit des données personnelles :

- l'article 9 de la convention n° 108 du Conseil de l'Europe, qui énonce qu'il est possible, en substance, de déroger à la quasi-totalité des dispositions protégeant les données personnelles lorsqu'une telle dérogation est considérée comme nécessaire, dans une société démocratique, à la préservation « des intérêts monétaires de l'État » ;
- l'article 13 de la directive 95/46, qui reprend cette exception précédemment rappelée, en précisant que de telles limitations à la protection des personnes fichées peuvent être justifiées par la nécessité de sauvegarder un intérêt économique de l'État, y compris dans le domaine fiscal ;
- le point n° 58 du préambule de cette même directive, ainsi que son article 69, qui énoncent que l'échange international de données personnelles entre administrations fiscales constitue une exception légitime au principe d'interdiction des flux transfrontières de données vers des États considérés comme n'ayant pas de protection adéquate de ces données.

[3] Directive 95/46/CE 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 du 23/11/1995, p. 31.

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119, 4.5.2016, pp. 1–88 (ci après « RGPD »).

Là où les textes internationaux relatifs à l'encadrement des traitements de données personnelles ouvrent potentiellement la porte à un certain nombre de dérives, la France a choisi une option relativement raisonnable. En effet, le législateur français n'a choisi d'inscrire au sein de la loi « informatique et libertés » qu'un nombre limité de ces exceptions :

– l'article 27, II de cette loi autorise la création de tout fichier fiscal (hors cas des interconnexions) par arrêté de l'administration concernée, pris après un avis publié et motivé de la CNIL. Tel est par exemple le cas de la délibération n° 2016-210 du 7 juillet 2016 de cette AAI, portant avis sur la modification du traitement « ADONIS » relatif à l'accès au dossier fiscal des particuliers. Cela signifie en clair que l'intervention de la CNIL n'est en rien bloquante et qu'en dépit de ses réserves éventuelles, un fichier peut être mis en œuvre alors qu'il ne présenterait pas toutes les garanties exigées par la loi du 6 janvier 1978 ;

– l'article 38, deuxième alinéa, de la loi informatique et liberté permet à l'administration fiscale, lorsqu'elle crée un nouveau traitement, de supprimer légalement la possibilité de s'opposer à ce traitement (« Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement »).

La spécificité de la protection des données personnelles en matière fiscale tient donc à ce que des dispositions protectrices des droits fondamentaux de la personne se trouvent en tout ou partie mises en échec pour un motif d'intérêt général. En soi, cela n'est ni nouveau ni spécifique, et l'on trouverait une problématique similaire toutes les fois où l'intérêt supérieur de l'État commande une atténuation légitime des droits et libertés.

En réalité, la vraie spécificité de la protection des données personnelles en matière fiscale tient en un mot : complexité. Les points de rencontre entre ces deux domaines paraissent extraordinairement délicats car ils nécessitent d'articuler deux ensembles réglementaires très différents et très sophistiqués. Et fatalement, l'accroissement des points de rencontre entre ces deux domaines est source d'incompréhension, voire d'incertitudes juridiques sérieuses pour les dispositions adoptées par l'administration fiscale. Si l'administration fiscale n'arrive pas à intégrer la complexité du droit des données personnelles, elle devra faire face sous peu à deux types de risques majeurs :

– le risque d'atteinte aux droits et libertés de la personne humaine en premier lieu, par l'atteinte aux droits au respect de la vie privée et à la protection des données personnelles, respectivement articles 7 et 8 de la Charte des droits fondamentaux de l'UE ;

– le risque portant sur la sécurité juridique des traitements mis en œuvre par l'administration fiscale, confrontée dans ce cas de figure aux conséquences délétères d'une annulation contentieuse de l'acte organisant un traitement de données personnelles.

C'est ce que nous avons choisi d'illustrer avec le traité FATCA[5], organisant l'échange automatisé de données personnelles fiscales entre la France et les États-Unis. Nous espérons, par cet exemple, attirer l'attention des spécialistes du droit fiscal sur cette discipline, le droit des traitements de données personnelles, dont le non respect menace directement un certain nombre de textes régissant la matière fiscale.

L'exemple du traité FACTA

Lorsque l'on examine la conformité juridique de cette convention aux standards européens du droit des données personnelles, une première question préalable se pose : La réglementation relative aux traitements de données personnelles est-elle matériellement applicable à cet accord ? Oui car elle s'applique à toute opération (collecte, échange, consultation, suppression, duplication etc.) portant sur des informations relatives à une personne directement ou indirectement identifiable. Nul ne contestera que le caractère de données personnelles aux informations relatives à des comptes bancaires (existence d'un compte dans tel ou tel organisme financier, montant des avoirs etc.). Nul ne contestera également qu'un transfert de ces données d'un établissement financier vers l'administration fiscale américaine constitue un traitement de données personnelles.

Une deuxième question préalable suit logiquement la première : la réglementation relative aux

[5] Décret n° 2015-1 du 2 janvier 2015 portant publication de l'accord entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et de mettre en œuvre la loi relative au respect des obligations fiscales concernant les comptes étrangers (dite « loi FATCA ») (ensemble deux annexes), signé à Paris le 14 novembre 2013, JORF n°0002 du 3 janvier 2015, page 86, texte n° 8.

traitements de données personnelles est-elle géographiquement applicable à cet accord ? L'article 5, I de la loi informatique et libertés énonce que « Sont soumis à la présente loi les traitements de données à caractère personnel : 1° Dont le responsable est établi sur le territoire français. (...) ». Or, c'est manifestement le cas des établissements financiers français, auxquels l'on demande de procéder à un traitement de données personnelles, en l'espèce un transfert.

Il importe également de préciser que la réglementation tant nationale qu'européenne (directive 95/46 et RGPD) n'exige aucune condition de nationalité pour l'application de leurs dispositions. Toute personne physique située sur le territoire européen bénéficie automatiquement de leurs garanties. En l'espèce, que les données personnelles soient relatives pour l'essentiel à des contribuables américains n'a pas d'incidence sur l'applicabilité de cette réglementation, et ce sans qu'il n'y ait même besoin d'évoquer les cas pas si rares de contribuables ayant la double nationalité française et américaine.

L'applicabilité de cette réglementation des traitements de données personnelles à la convention FATCA implique sa soumission aux dispositions de la loi informatique et libertés, qui transpose la directive 95/46. Il convient de préciser que les dispositions de cette dernière ont fait l'objet, assez récemment, d'une interprétation très rigoureuse de la part de la CJUE. Il ne suffit donc pas à un traitement de données personnelles de respecter les textes idoines pour être en conformité, il doit l'être également avec les obligations jurisprudentielles en la matière.

Or, en l'espèce, quelles sont les obligations afférentes à un transfert de données personnelles de la France vers les États-Unis ?

On parle de transfert de données à caractère personnel lorsque ces données sont transférées depuis le territoire européen vers un État ou une organisation internationale qui n'appliquent pas les dispositions de la directive 95/46/CE. Le transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (par exemple : par accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (exemple d'un disque dur d'ordinateur à un serveur, ou du franchissement physique d'une frontière par une clef usb contenant des données personnelles). Le transfert doit être volontaire, il ne peut consister en une simple mise à disposition d'informations sur un site web[6].

Un transfert ne peut avoir lieu « vers un État n'appartenant pas à la Communauté européenne que si cet État assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet »[7]. Toutefois, l'article 69 de cette même loi autorise de tels transferts dans un nombre limité de cas : « le responsable d'un traitement peut transférer des données à caractère personnel vers un État ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes : (...) 2° À la sauvegarde de l'intérêt public ; (...) ». À la lecture de ces lignes, l'on pourrait alors se dire que le traité FATCA respecte bien la loi Informatique et libertés car la lutte contre l'évasion fiscale qu'organise ce traité relève manifestement de l'intérêt public.

C'est également à notre sens l'analyse qu'ont du faire les auteurs de cette convention. Ils ont juste totalement méconnu l'existence d'obligations jurisprudentielles qui encadrent impérativement toute opération de traitement de données personnelles.

En effet, lorsque la CJUE examine un point en matière de droit des traitements de données personnelles, elle interprète systématiquement l'ensemble des dispositions existantes, même les plus techniques, à la lueur des droits fondamentaux[8]. Dans le cadre de cette attention particulière aux droits fondamentaux, la jurisprudence de la CEDH a constitué une source d'inspiration nettement privilégiée, ce dont a témoigné et témoigne encore l'article 6 du Traité sur l'UE. Cette révérence à la jurisprudence de la CEDH s'est également traduite par une reprise et une synthèse des exigences générales de sa jurisprudence au sein de la Charte des droits fondamentaux de l'UE, en cas de violation d'un droit garanti par la CESDH. Cette Charte comporte donc, outre un article 8 garantissant à toute personne la protection de ses données personnelles, un article 52, 1 qui énonce des limites précises et claires à toute limitation des droits garantis par cette Charte[9].

Ces précisions préalables étant rappelées, la position de la CJUE est qu'un traitement de données personnelles constitue, en jurisprudence, une violation par principe du droit à la protection des données personnelles au sens de l'article 8 de la Charte[10]. La CEDH ne procède pas autrement, qui considère de longue date qu'un traitement de données personnelles constitue par

[6] CJCE 6 novembre 2003, aff. C 101/01, *Bodil Lindqvist*.

[7] Loi informatique et libertés, art 68.

[8] voir CJCE 20 mai 2003, aff. C 465/00, *Osterreischicher Rundfunk*, § 68 : « Il y a lieu encore d'ajouter que les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante, font partie intégrante des principes généraux du droit dont la Cour assure le respect (voir, notamment, arrêt du 6 mars 2001, Connolly/Commission, C-274/99 P, Rec. p. I-1611, point 37).

[9] Charte des droits fondamentaux de l'UE, art 52,1 : « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

[10] CJUE 8 avril 2014, aff. C 293/12, *Digital Rights* : § 36 : « De même, la directive 2006/24 est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'elle prévoit un traitement des données à caractère personnel ».

principe une nuisance au droit au respect de la vie privée de la personne humaine, indépendamment des caractéristiques du traitement ou des données en cause[11].

Pour autant, tant la jurisprudence européenne que les textes s'accordent également sur le fait que le droit à la protection des données personnelles ne constitue pas un droit absolu. Ainsi, dans le texte de la CESDH, l'article 8 relatif au droit au respect de la vie privée énonce, dans son premier paragraphe, le principe de non-ingérence des autorités publiques dans l'exercice du droit à la vie privée, et admet, dans son deuxième paragraphe, qu'une telle ingérence est possible pour autant qu'elle soit « *prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui*». Le RGPD le rappelle tout aussi clairement, dans le considérant n° 4 de son préambule : « *Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité* ».

Il est donc juridiquement possible de porter atteinte aux règles de protection des données personnelles pour autant que soient respectés les critères établis par la CEDH et synthétisés à l'article 52 §1 de la Charte des droits fondamentaux. Dans ce cadre, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit cumulativement :

– être prévue par la loi ;
– respecter leur contenu essentiel ;
– être nécessaire et proportionnée à une finalité légitime comme la poursuite d'un objectif d'intérêt général ou la protection des droits et libertés d'autrui.

Donc, pour évaluer la légalité d'un traitement de données personnelles au droit éponyme, quelque soit ce traitement, il faut, en plus de respecter l'économie des normes écrites, se poser quatre questions relatives à l'acte ou au comportement considéré comme litigieux :

– le principe de sécurité juridique est-il respecté ?
– certaines des garanties du droit fondamental considéré sont-elles purement et simplement niées ?
– existe-t-il un intérêt permettant de racheter la violation de ce droit ?
– une violation de ce droit fondamental est-elle strictement nécessaire à l'accomplissement de cet intérêt supérieur ?

La CJUE a donné un exemple assez récent d'utilisation de cette grille en matière de droit des traitements de données personnelles, exemple qu'il convient d'avoir à l'esprit pour juger de la conformité juridique du traité FATCA. Tout part d'une question en apparence technique, celle de la conformité des procédés de *Safe harbor* américains au droit de l'UE relatif aux traitements de données personnelles[12]. Le requérant, Maximilian Schrems, demandait à l'équivalent irlandais de la CNIL d'examiner la légalité des transferts de données personnelles le concernant effectuée par *Facebook* de l'Irlande – où elle a concentré ses services européens – vers les États Unis – où elle a son siège social et ses centres de données. Plus précisément, de tels transferts ne lui paraissaient pas conformes à l'exigence posée par l'article 25 de la directive 95/46 du 24 octobre 1995 que de telles exportations de données soient subordonnées, dans l'État d'importation, à l'existence d'un niveau adéquat de protection des données personnelles.

L'essentiel de l'affaire tournait donc autour de la façon dont doit s'interpréter la directive 95/46, et notamment son article 25, pour fonder en droit les transferts de données personnelles à destination d'États tiers à l'UE. Cette disposition subordonne le transfert de données personnelles de citoyens européens hors de l'UE à l'existence, au sein de l'État vers lequel ces données sont exportées, d'un « niveau de protection adéquat ». Les critères permettant d'apprécier cette adéquation sont compris de manière large par cette directive[13] et peuvent faire l'objet d'une appréciation officielle de la part de la Commission. Dans ce dernier cas, celle-ci prend une décision pour reconnaître, s'il y a lieu, l'adéquation du standard de protection de l'État tiers[14], permettant ainsi aux flux de données personnelles d'y être exportés[15]. En tant que tels, les États-Unis n'ont jamais fait l'objet d'une telle reconnaissance par la Commission européenne.

Au terme de l'article 25, al. 2 de la directive 95/46 précitée, une décision de la Commission peut intervenir pour constater l'existence d'un niveau de protection adéquat au sein d'un État tiers. L'appréciation doit donc porter de manière globale sur la façon dont l'État en question réglemente les traitements de données personnelles. Or, la décision servant de base juridique aux trans-

[11] CEDH du 16 février 2000, Amann c/Suisse, §68 et 69.

[12] CJUE, gr. ch., 6 octobre 2015, aff. C-362/14, *Maximillian Schrems c/ Data Protection Commissioner*.

[13] Directive 95/46, article 25, al. 2 : « Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées. »

[14] Directive 95/46, art. 25, al. 6.

[15] Voir par exemple Décision 2011/61/UE de la Commission du 31 janvier 2011 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'État d'Israël concernant le traitement automatisé des données à caractère personnel [notifiée sous le numéro C(2011) 332].

ferts de données personnelles de l'UE vers certaines grandes entreprises américaines, la décision 2000/520/CE de la Commission du 26 juillet 2000[16] n'attribuait un tel label d'adéquation non pas à ce pays tiers que sont les États-Unis d'Amérique, mais seulement à un procédé d'autorégulation, les *Safe Harbor*. Ce procédé, inspiré du droit boursier américain, visait à garantir au sein des entreprises qui y adhéraient volontairement un degré de protection des données personnelles purement et simplement basé sur l'autorégulation.

La CJUE a conclu à la non-conformité de la décision 2000/520 reconnaissant l'adéquation des *Safe Harbor* à la directive 95/46 et a prononcé son invalidation pour trois motifs. Premièrement parce que cette décision aboutissait à une ingérence dans le droit fondamental garanti à l'article 8 de la Charte des droit fondamentaux de l'UE, ingérence non limitée au strict nécessaire, du fait de la collecte de masse des données opérée (§§92-93). Deuxièmement parce que les dispositions relatives aux *Safe Harbor* ne prévoyaient pas, pour une personne dont les données seraient traitées, la possibilité d'exercer un recours juridictionnel, niant ainsi la substance du droit à une protection juridictionnelle effective garanti dans l'article 47 de la Charte.

Enfin, et c'est ce dernier argument que nous devons retenir à l'esprit pour évaluer la conformité du FATCA aux standards européens du droit des données personnelles, la Cour a considéré que « la décision 2000/520 ne comporte aucune constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale. (…). À cela s'ajoute le fait que la décision 2000/520 ne fait pas état de l'existence d'une protection juridique efficace contre des ingérences de cette nature. (...) » (§§88 et 89).

De cette décision nous pouvons déduire deux éléments :

– les États-Unis ne constituent pas un État que la CJUE regarde comme assurant un degré de protection suffisant des données personnelles, loin s'en faut. Il faut à cet égard noter que les *Safe Harbor* ont depuis été remplacés par un autre accord validé par une décision de la Commission européenne, le *Privacy Shield*, qui fait l'objet de recours actuellement pendants devant un certain nombre de juridictions d'États membres de l'UE ;

– un acte juridique organisant un transfert de données d'un État de l'UE vers les États-Unis doit clairement indiquer en son sein, de manière claire et accessible, les garanties prévues pour assurer un minimum de protection des données personnelles.

Or, que constate-t-on lorsque l'on examine le texte du FATCA ? Que cette convention qui organise un échange automatisé de données personnelles de citoyens potentiellement français à destination des États-Unis comporte comme seule garantie des droits fondamentaux des personnes concernées, un article 3, 7 libellé ainsi : « Tous les renseignements échangés sont soumis aux obligations de confidentialité et autres protections prévues par la Convention, y compris aux dispositions qui limitent l'utilisation des renseignements échangés ». Autant dire qu'il n'existe littéralement aucune disposition permettant à un contribuable français de se faire une idée même vague du sort de ses données personnelles si jamais ces dernières faisaient l'objet d'un transfert outre-Atlantique.

Dans ces conditions, l'impératif de sécurité juridique clairement exposé à l'article 52, 1 de la Charte des droits fondamentaux de l'UE n'est pas respecté. Le FATCA, traité organisant de manière automatisée l'échange de données fiscales entre la France et les États-Unis, est donc entaché d'une irrégularité grossière devant logiquement conduire à son annulation. Et derrière le FATCA, se trouve, dans une posture similaire, toute convention qui organiserait l'échange automatisé de données personnelles entre un État de l'UE et un État extra-européen. Par exemple l'Accord multilatéral entre autorités compétentes concernant l'échange de déclarations pays par pays[17].

Au final, la spécificité de la protection des données personnelles en matière fiscale tient à la complexification de l'élaboration de la norme fiscale, qui ne pourra plus se permettre bien longtemps d'ignorer les exigences de cette réglementation exotique. À défaut de quoi, la norme fiscale, lorsqu'elle abordera la question des traitements de données, fera systématiquement planer un risque réel pour la protection des données personnelles des citoyens et, par ricochet, un risque sur la sécurité juridique des actes qui ignoreraient les obligations imposées par la loi informatique et libertés, la directive 95/46 et, demain, par le Règlement général sur la protection des données. ■

[16] 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 L215 du 25 08 2000, p. 7.

[17] Décret n° 2017-672 du 28 avril 2017 portant publication de l'accord multilatéral entre autorités compétentes portant sur l'échange des déclarations pays par pays, signé à Paris le 27 janvier 2016