JURAJ SCHWARCZ[*]

Protection des données à caractère personnel dans l'Union européenne

Introduction

C'est pour moi un grand honneur que de pouvoir contribuer au Liber Amicorum dédié à M. le professeur Czúcz à l'occasion de son 70[e] anniversaire et de sa longue carrière scientifique, professorale, et en tant que juge européen. C'est d'ailleurs dans ces fonctions, au sein du Tribunal de l'Union européenne à Luxembourg, que nous nous sommes rencontrés pour la première fois. J'ai pu côtoyer M. le professeur Czúcz régulièrement, que ce soit durant les conférences plénières, au cours de discussions juridiques ou même, de manière purement amicale, à l'occasion de rencontres autour d'un café ou d'un déjeuner. Quel qu'ait été le lieu de ces entrevues, et quel que puisse avoir été le sujet de nos conversations, j'en garde le meilleur souvenir. En effet, M. le professeur fait partie de ce cercle très restreint de personnes qui, dans tous les domaines de discussion, fait montre non seulement de connaissances profondes, d'érudition, de bon sens, mais également de calme et de retenu, en d'autres termes, des qualités indispensables à tout professeur ou juge. Je ne peux m'empêcher d'ajouter qu'un lien existe entre nous, en effet nous pouvons communiquer dans une langue qui nous est chère, à savoir, sa langue maternelle, le hongrois. Cela nous permet quelquefois de nous éloigner de notre quotidien, et ainsi d'évoquer, en aparté, nos pays respectifs, la Hongrie et la Slovaquie, pays voisins, dont l'amitié et le respect mutuel sont, je l'espère, aussi forts que ce lien qui nous uni. C'est dans ces circonstances que je voudrais, une fois encore, lui souhaiter tout le meilleur pour son anniversaire, en ajoutant quelques humbles considérations sur l'un des sujets qui nous préoccupe souvent, à savoir, le respect de la Charte de l'Union européenne. Sur ce point, c'est un aspect très particulier qui me tient à cœur - la protection des données à caractère personnel.

[*] JUDr., PhD, juge au Tribunal de l'Union européenne – Je tiens à remercier Mgr. A. Stec pour son aide précieuse lors de la rédaction de cet article.

Charte des droits fondamentaux de l'Union européenne[1]

Préambule

« Les peuples de l'Europe, en établissant entre eux une Union sans cesse plus étroite, ont décidé de partager un avenir pacifique fondé sur des valeurs communes.

Consciente de son patrimoine spirituel et moral, l'Union se fonde sur les valeurs indivisibles et universelles de dignité humaine, de liberté, d'égalité et de solidarité; elle repose sur le principe de la démocratie et le principe de l'État de droit. Elle place la personne au cœur de son action en instituant la citoyenneté de l'Union et en créant un espace de liberté, de sécurité et de justice.

L'Union contribue à la préservation et au développement de ces valeurs communes dans le respect de la diversité des cultures et des traditions des peuples de l'Europe, ainsi que de l'identité nationale des États membres et de l'organisation de leurs pouvoirs publics au niveau national, régional et local; elle cherche à promouvoir un développement équilibré et durable et assure la libre circulation des personnes, des biens, des services et des capitaux, ainsi que la liberté d'établissement.

À cette fin, il est nécessaire, en les rendant plus visibles dans une Charte, de renforcer la protection des droits fondamentaux à la lumière de l'évolution de la société, du progrès social et des développements scientifiques et technologiques. […] »

[…]

Chapitre ii
Libertés

[…]

« Article 8

Protection des données à caractère personnel

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. »

[1] JO 2000, C 364, p. 1;

Contexte historique et actuel des droits fondamentaux

Tout d'abord, rappelons que jusqu'à la proclamation de la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), le 7 décembre 2000, seuls les initiés étaient en mesure de connaître l'étendue et l'intensité de la protection des droits de la personne au sein d'un espace trop souvent considéré uniquement au sens économique. En effet, si, depuis le milieu des années 1960, sur la base d'un dialogue fructueux avec les juridictions constitutionnelles allemande et italienne, la Cour de justice de l'Union européenne[2] a élaboré un catalogue des droits fondamentaux consacrés en tant que principes généraux du droit communautaire, dont elle assurait le respect que ce soit dans le contexte des actions des institutions européennes ou lorsque les États membres mettaient en œuvre le droit de la Communauté, il ne s'agissait que d'une construction prétorienne, inconnue des citoyens européens. Ce n'était qu'après l'adoption de la Charte que le processus d'évolution d'une intégration essentiellement économique vers une intégration plus politique, incluant l'idéal d'un espace érigeant la protection des droits comme référence, fut réellement entamé.[3]

La Charte est un texte important, tout autant par son contenu que par son processus d'élaboration et sa destinée, comme cela a été amplement analysé dans la doctrine[4]. Elle constitue un élément indispensable dans la logique de recherche d'une légitimité de l'Union en quête d'une identité politique. L'on ne saurait suffisamment mettre en exergue l'importance d'un tel catalogue de droits fondamentaux, propre à l'Union, en particulier en tenant compte des différentes avancées dans la construction de cette dernière et qui se voit attribuée de plus en plus de compétences dans des domaines relativement diversifiés. La Charte a été adoptée dans un environnement juridique européen dans lequel existait déjà un ensemble de normes protégeant les droits fondamentaux, incluant des instruments tels que la Convention européenne des droits de l'homme (ci-après la « Convention ») ou les différentes constitutions nationales. C'est par le biais d'une coexistence entre ces différents instruments que l'Europe garantie effectivement un haut degré de protection des droits fondamentaux.[5] De surcroît, il est envisagé de modifier encore quelque peu ce cadre complexe, dès lors que, comme cela ressort de l'article 6, paragraphe 2, du Traité sur l'Union européenne (ci-après « TUE »), il est imposé à l'Union d'adhérer à la Convention, le protocole n° 8 indiquant que cette adhésion doit se faire dans le respect des spécificités de l'Union. Cependant, sur ce dernier point, force est de constater que, alors même que les négociations ouvertes entre l'Union et le Conseil de l'Europe ont abouti à un projet d'accord d'adhésion qui avait été soumis par la Commission à la Cour de justice, en application de l'article 218, paragraphe 11, du Traité sur le fonctionnement de l'Union (ci-après « TFUE »), la procédure a été ralentie à la suite de l'avis 2/13 de la Cour, datant du 18 décembre 2014, selon lequel il y a incompatibilité d'accord avec l'article 6, paragraphe 2, TUE et le protocole n° 8 relatif à cet article.

---

[2] Initialement dénommée la Cour de justice des Communautés européennes

[3] Voir, en ce sens, Andriantsimbazovina, J., GAUDIN, H., MARGUÉNAUD, J-P., RIALS, S., SUDRE, F., *Dictionnaire des Droits de l'Homme*. Presses Universitaires de France, 2008, p. 127.

[4] Voir, à titre d'exemple, S. PEERS, T. HERVEY, J. KENNER, A. WARD, *« The EU Charter of Fundamental Rights »;* également, Andriantsimbazovina. J., GAUDIN, H., MARGUÉNAUD, J-P., RIALS, S., SUDRE, F., *op.cit*, p. 128 et 129.

[5] Voir également. PEERS, S., HERVEY, T., KENNER, J., WARD, A.: *The EU Charter of Fundamental Rights*, notamment la préface de M. V. Skouris, ancien président de la Cour de justice.

Du rôle important de la Cour de justice et du Tribunal

Si, sur ce dernier point, l'avancée prévue par le TUE est donc, pour ainsi dire, « mise en attente », il convient de rappeler que, dans une multitude d'autres situations qui se sont présentées sur le plan des droits fondamentaux, ladite Cour a procédé à des avancées permettant d'affirmer qu'actuellement, tant au niveau législatif qu'au niveau jurisprudentiel, l'Union accorde l'un des niveaux les plus élevés de protection. Cette constatation demeure valable même si nous la comparons à celle d'autres régions du monde, dans lesquelles les droits de l'homme sont traditionnellement bien respectés. À titre d'exemple, nous pouvons citer les arrêts de la Cour du 18 juillet 2013, Commission e.a./Kadi, (C-584/10 P, C-593/10 P et C-595/10 P, Rec, EU:C:2013:518), ou du 21 décembre 2011, France/People's Mojahedin Organization of Iran, (C-27/09 P, Rec, EU:C:2011:853), ce dernier confirmant l'arrêt du Tribunal du 4 décembre 2008, People's Mojahedin Organization of Iran/Conseil, (T-284/08, Rec, EU:T:2008:550).

Avancées concrètes dans la protection des données à caractère personnel

Dans le domaine de la protection de données personnelles – qui nous intéresse plus particulièrement dans cet article[6] – nous pourrions citer des arrêts de principe récents, comme ceux du 8 avril 2014, Commission/Hongrie, (C-288/12, Rec, EU:C:2014:237), du 8 avril 2014, Digital Rights Ireland e.a., (C-293/12 et C-594/12, Rec, EU:C:2014:238), ou du 13 mai 2014, Google Spain et Google, (C-131/12, Rec, EU:C:2014:317)[7]. Le premier arrêt susmentionné a permis à la Cour de justice de se prononcer sur une situation, dans laquelle la Hongrie avait mis fin, de manière anticipée, au mandat du commissaire chargé de la protection des données. Cette affaire portait sur l'interprétation de la 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[8], conformément à laquelle les États membres devaient, notamment, désigner une ou plusieurs autorités chargées de veiller au respect des règles de ladite directive sur leur territoire, et ce en exerçant leurs fonctions en toute indépendance[9]. La Cour a jugé, en substance, qu'une telle « indépendance » de

[6] Ladite protection ayant été renforcée, au niveau européen, en particulier à la suite de l'adoption du traité de Lisbonne, grâce auquel la Charte est devenue un document juridiquement contraignant (voir notamment, l'article 16 TFUE et, par référence, l'article 39 TUE).

[7] Si nous visions à rappeler même certains arrêts plus anciens, il conviendrait certainement d'inclure, par exemple, l'arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, Rec, EU:C:2003:294, qui tendait à clarifier le champ d'application de la directive 95/46/CE;

[8] JO L 281, p. 31

[9] Voir, notamment, l'article 28, paragraphe 1, de la directive citée (JO L 281, p. 31). Comme constaté par la Cour au point 47 de l'arrêt cité, l'exigence de contrôle par une autorité indépendante du respect des règles de l'Union relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel résulte également du droit primaire de l'Union, notamment de l'article 8, paragraphe 3, de la charte des droits fondamentaux de l'Union européenne et de l'article 16, paragraphe 2, TFUE; Par ailleurs, l'article 8 de la Charte est basé, également, sur l'article 8 de la Convention européenne des droits de l'homme et s'inspirait du règlement (CE) n° 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère

l'autorité de contrôle incluait nécessairement l'obligation, imposée aux États membres, de respecter la durée du mandat qui lui fut confié. Plus particulièrement, elle a rappelé que les autorités de contrôle créées conformément à la directive devaient pouvoir exercer leurs missions sans aucune influence extérieure. Selon la Cour, cela impliquait qu'elles ne pouvaient être liées par aucune instruction dans l'exercice de leurs fonctions et, de surcroît, qu'il leur incombait de décider sans aucune influence politique – le risque même d'une telle influence devait, d'ailleurs, être écarté. Or, selon la Cour, précisément le fait de permettre à un État membre de mettre fin au mandat d'une autorité de contrôle avant son expiration, sans respecter les règles et les garanties préétablies à cette fin par la législation applicable, pourrait conduire celle-ci à obéir à la volonté du pouvoir politique.

S'agissant des deux arrêts Digital Rights Ireland e.a., et Google Spain et Google, précités, ils concernent, quant à eux, la société de l'information. Rappelons, avant d'en venir à leur analyse concrète, le contexte général. Il ressort d'une étude relativement récente, effectuée par la Commission et visant à connaître les opinions des citoyens de l'Union quant à la protection des données à caractère personnel dans un environnement numérique[10], tout d'abord, que leur confiance envers un tel environnement est très basse. Ainsi, deux tiers des personnes ayant fait l'objet de l'enquête (67 %) ont affirmé qu'elles étaient consternées par l'absence de contrôle sur les informations qu'elles communiquaient en ligne. Seul 15 % des personnes ayant répondu aux demandes ont indiqué avoir l'impression d'un contrôle complet. Il est, également, important de noter que 63 % n'avaient pas confiance dans le commerce électronique, de manière générale, et 62 % manquaient de confiance par rapport aux entreprises de télécoms ou même vis-à-vis des prestataires de services Internet. Les problèmes soulevés incluaient la question de savoir de quelle manière étaient utilisées, en réalité, les données personnelles collectées – 70 % des personnes interrogées estimaient que c'était à des fins différentes de celles pour lesquelles la collecte avait initialement été effectuée. Une majorité de l'opinion estimait que la protection des données à caractère personnel ne devait être limitée aux frontières, mais, au contraire, qu'elle devait être équivalente indépendamment de l'autorité ou de l'entreprise gérant ces données. Enfin, la Commission a mis en avant la nécessité d'une réforme, consistant en une modernisation du cadre juridique dans le contexte de la création du marché numérique unique, afin de gagner en cohérence et par là même la confiance des citoyens européens.

Plus concrètement, le paquet relatif à la réforme sur la protection des données s'articule autour de deux projets législatifs: un règlement général qui couvre l'essentiel du traitement des données personnelles au sein de l'Union et une directive sur la protection des données qui vise à prévenir, détecter ou poursuivre les infractions pénales ainsi qu'à les sanctionner. Le projet de règlement met à jour les principes établis dans la directive de 1995, afin de suivre le rythme des principaux changements dans le secteur du traitement des données, nés avec Internet. Il couvrirait par exemple les données traitées sur Internet, telles que pour les

personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8, p. 1.); ce dernier règlement avait notamment instituée l'autorité de contrôle indépendante, dénommée « Contrôleur européen de la protection des données ». Enfin, conformément à la note explicative à l'article 8 de la Charte, celui-ci a encore pris pour base la Convention du Conseil de l'Europe, du 28 janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

[10] Eurobaromètre, datant du 24 juin 2015 (http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm)

réseaux sociaux, le commerce en ligne et les services bancaires[11]. La proposition de directive devrait remplacer une décision-cadre datant de 2008 sur le traitement transfrontalier des données en matière de coopération policière et judiciaire. Son objectif est de mieux protéger les transferts de données nationaux et transfrontaliers. Le but est également d'assurer un haut niveau de protection des données pour les citoyens.

Contexte actuel, particulièrement difficile – régression future dans le domaine de la protection des données à caractère personnel, voir, dans celui des droits fondamentaux?

Cependant, force est de constater que, dans le contexte actuel, la question de la recherche d'un réel équilibre entre, d'une part, la protection des données personnelles et, d'autre part, les actions nécessaires aux fins d'assurer la sécurité en Europe suite aux événements récents, notamment à Paris en janvier et novembre 2015, est devenue, pour des raisons évidentes, encore plus épineuse qu'auparavant. Notons que, très récemment, la Commission européenne a promis, ainsi que le Conseil européen, une accélération des discussions portant sur le « Passenger Name Record (registre des noms de passagers) » (ci-après juste le « PNR »)[12]. Ledit PNR constitue un projet de vaste fichier recensant l'identité de tous les passagers des avions circulant, entrant ou sortant de l'espace européen. Les données seraient conservées durant cinq ans. Il prévoit que les services de renseignement européens puissent accéder à ce vaste fichier, mais donnerait également accès à ces données à certains pays alliés, au premier chef les États-Unis[13]. Par le passé la commission « libertés civiles, justice et affaires intérieures » du Parlement européen avait réussi à bloquer le projet. Le scandale des programmes de surveillance de masse de la NSA américaine, révélés par E. Snowden, était venu renforcer le camp des opposants. Cependant, le projet a été relancé suite aux évènements susvisés, ayant récemment eu lieu à Paris. Il convient d'ajouter que plus de la moitié des États européens se sont déjà dotés de PNR nationaux, dont le défaut majeur demeure, à ce stade, qu'ils ne sont pas interconnectés de sorte à être réellement utiles dans un contexte ou la criminalité et le terrorisme sont internationalisés[14]. Enfin, notons que dans les circonstances particulières liées à la recherche d'une solution sécuritaire, la France a récemment informé le Conseil de l'Europe « de sa décision de déroger à la Convention européenne des droits de l'homme », du fait de l'adoption de l'état d'urgence après les

[11] http://www.europarl.europa.eu/news/fr/newsroom/content/20130502BKG07917/html/QuestionsR%C3%A9ponses-sur-la-r%C3%A9forme-du-r%C3%A9gime-de-protection-des-donn%C3%A9es-de-l'UE

[12] Voir, par exemple, *« Lutte contre le terrorisme: qu'est-ce que le PNR, le fichier sur les passagers aériens? »,* dans le journal Le Monde, du 26 novembre 2015 (http://www.lemonde.fr/international/article/2015/11/19/qu-est-ce-que-le-pnr_4813315_3210.html); également, S. MAKTOUF: « *Conseil auprès de la Cour Pénale Internationale* », notamment sur le « PNR européen ou planétaire »; Le Figaro, 25 novembre 2015.;

[13] Après les attentats du 11 septembre 2001, les États-Unis avaient exigé que les Européens leur communiquent les données personnelles des passagers des vols transatlantiques, et les intègrent dans leur propre base de données de passagers. Après une longue bataille diplomatique et juridique, les États-Unis finissent par l'emporter: en avril 2012, le Parlement européen ratifie l'accord PNR euro-américain.

[14] « Lutte contre le terrorisme: qu'est-ce que le PNR, le fichier sur les passagers aériens? », Le Monde, du 26 novembre 2015; également, « Attentats: le PNR changera-t-il vraiment la donne? », Les Echos, 23 novembre 2015, portant notamment sur la question « des voyages avec de vrais papiers sous un faux nom » http://www.lesechos.fr/politique-societe/societe/021501844427-attentats-le-pnr-changera-t-il-vraiment-la-donne-1177787.php

attentats du 13 novembre 2015[15]. En réponse, le Conseil de l'Europe a prévenu que, alors que certaines mesures envisagées par la France étaient susceptibles de nécessiter une dérogation à certains droits garantis par ladite Convention, cette dernière restait en vigueur en France, avec d'autres droits qui ne pourront tolérer de dérogation.[16] La notification de cette dérogation est prévue à l'article 15 de la Convention européenne des droits de l'homme: en « *cas de guerre ou d'autre danger public menaçant la vie de la nation* », un État signataire « *peut prendre des mesures dérogeant aux obligations* » de la convention, sous réserve d'en informer le Conseil de l'Europe.[17.] D'autres États membres ont exercé ce droit de dérogation, comme le Royaume-Uni, après les attentats de juillet 2005. Ainsi, comme tant de fois dans l'histoire de l'humanité, nous nous trouvons dans un contexte où les libertés semblent être, à tort ou à raison, limitées pour des raisons de sécurité.[18] Si une approche sécuritaire est d'actualité dans plusieurs pays et constitue, entre autres, une réaction aux événements récents, encore faut-il que l'empilement législatif qui en découle permette d'atteindre une réelle efficacité au regard des menaces subies. Une analyse de différents moyens mis en œuvre, et la recherche d'un équilibre tenable avec les droits et libertés, est particulièrement important dans ce contexte – notons, à titre d'exemple, que le FBI a annoncé, en mai 2015, qu'aucune affaire sérieuse de terrorisme n'avait été résolue grâce à la section « 215 » du Patriot Act, une des plus controversée, qui permet la collecte en masse d'informations privées. Même en France, après l'adoption de la loi relative au renseignement du 24 juillet 2015, qui étendait drastiquement les pouvoirs de l'État au détriment des droits et des libertés fondamentaux (vie privée, absence de contrôle juridictionnel), la question était posée de savoir quelle était l'utilité précise de cette loi, dans un contexte où il semble que c'était plus l'analyse des informations obtenues que leur simple collecte qui laissait à désirer.[19] Ces questions relèvent, à ce stade, bien évidemment, de la compétence des législateurs concernés, auxquels il appartient de réagir, autant que possible, aux différentes menaces que présente le monde d'aujourd'hui, sans bafouer, concomitamment, les acquis dans la protection des droits fondamentaux, et, en particulier, le droit à la protection des données à caractère personnel.

---

[15] Voir, *« État d'urgence: la France envisage de déroger à la Convention européenne des droits de l'homme »*; Le Monde, 27 novembre 2015; http://www.lemonde.fr/attaques-a-paris/article/2015/11/27/etat-d-urgence-la-france-envisage-de-deroger-a-la-convention-europeenne-des-droits-de-l-homme_4819057_4809495.html

[16] Tel le droit à la vie et l'interdiction de la torture et des peines ou traitements inhumains ou dégradants;

[17] Ce ne sera, le cas échéant, que dans le contexte d'éventuelles requêtes précises, où la France serait défenderesse, que la Cour européenne des droits de l'homme aura à se prononcer sur la validité de cette dérogation;

[18] Voir, par exemple. GEARTY, C.: *« Struggling Towards the Universal (Liberty Captured by Security) »*; dans *Liberty & Security*, Polity Press, 2013, notamment p. 7, référence doit être faite, dans ces circonstances, à la locution « l'homme est un loup pour l'homme » (Homo homini lupus est), régulièrement utilisée que ce soit par Hobbes (De cive), Pline l'Ancien (*Histoire naturelle*), F. Bacon (De *Dignitate et augmentis scientiarum*), et bien d'autres encore.

[19] Voir, par exemple, *«Naissance et ascension d'une idéologie révolutionnaire: 35 ans d'islam politique violent»*,. CLÉMENT, P. A.: *Diplomation, Affaires stratégiques et relations internationales*. n° 77, novembre-décembre 2015, p. 39.

« Digital Rights Ireland e.a.» et « Google Spain e.a. »

Pour en revenir aux arrêts Digital Rights Ireland e.a., et Google Spain et Google, adoptés tous deux par la grande chambre de la Cour de justice, il convient de rappeler que par le premier, la Cour de justice a invalidé la directive n° 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive n° 2002/58/CE (JO L 105, p. 54). Cette directive avait, comme principal objectif, d'harmoniser les dispositions des États-membres portant sur la conservation de certaines données caractérisées. Elle visait, notamment, à garantir la disponibilité de ces données aux fins de prévention, de recherche, de détection et de poursuite des infractions graves, comme notamment des infractions liées à la criminalité organisée et au terrorisme. Il s'agissait ainsi de conserver des données relatives au trafic, à la localisation et d'autres données connexes nécessaires pour identifier l'abonné ou l'utilisateur. En revanche, il n'était pas question de conserver le contenu même de la communication et les informations consultées.

Les questions préjudicielles posées à la Cour de justice par la High Court (Haute Cour, Irlande), ainsi que par le Verfassungsgerichtshof (Cour constitutionnelle, Autriche), visaient, en substance, à ce que soit examinée la validité de cette directive à la lumière de certains droits fondamentaux garantis par la Charte, notamment le droit au respect de la vie privée et le droit à la protection des données à caractère personnel (articles 7 et 8 de la Charte). La Cour de justice a analysé, en détails, le régime prévu par la directive, et a tout d'abord constaté que les données collectées, prises dans leur ensemble, étaient susceptibles de fournir des indications très précises sur la vie privée des personnes concernées. Cela pouvait inclure des informations portant sur leurs habitudes quotidiennes, leurs lieux de séjours permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales et les milieux sociaux fréquentés. Ensuite, la Cour a mis en exergue le fait qu'est généré, dans l'esprit des personnes concernées, le sentiment que leur vie privée fait l'objet d'une surveillance constante, dans la mesure où la conservation et l'utilisation ultérieure des données sont effectuées sans qu'elles n'en soient informées. Tout en constatant qu'une telle ingérence dans les droits fondamentaux était justifiée, la Cour a considéré, toutefois, qu'en adoptant la directive en cause, le législateur de l'Union a excédé les limites qu'imposait le respect du principe de proportionnalité.

Sur ce dernier point, la Cour a considéré qu'il convenait de procéder à un contrôle strict, le pouvoir d'appréciation du législateur de l'Union s'avérant être réduit dans la mesure où, d'une part, la protection des données à caractère personnel jouait un rôle important au regard du droit fondamental au respect de la vie privée, et, d'autre part, tenant compte de l'ampleur et de la gravité de l'ingérence dans ce droit prévue par la directive. Or, la Cour a jugé que, précisément, cette ingérence n'était pas suffisamment encadrée afin de garantir sa limitation au strict nécessaire. Premièrement, la Cour a mis en avant le fait que l'ensemble des individus, des moyens de communication électronique et des données relatives au trafic étaient couverts, sans aucune différenciation, limitation ou exception. Deuxièmement, la directive ne prévoyait aucun critère objectif qui permettait de garantir que les autorités nationales compétentes ne pouvaient utiliser les données qu'aux seules fins de prévenir, détecter ou poursuivre pénalement des infractions

susceptibles d'être considérées, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux en question, comme suffisamment graves. Troisièmement, la Cour a critiqué le fait que la durée de conservation des données imposée était d'au moins six mois (voir, dans certains cas, pouvait atteindre 24 mois), sans opérer une quelconque distinction entre les catégories de données en fonction des personnes concernées et de l'utilité éventuelle des données par rapport à l'objectif poursuivi. Enfin, la Cour a critiqué le fait que la directive ne contenait pas de garanties de protection efficace contre les abus, permettait de décider du niveau de sécurité des données en fonction de certaines considérations économiques et, de surcroît, n'imposait pas non plus la conservation des données sur le seul territoire de l'Union. Ainsi, selon la Cour, cette directive ne garantissait pas pleinement le contrôle du respect des exigences de protection et de sécurité par une autorité indépendante, comme cela est pourtant exigé par la charte.

Le second arrêt susmentionné, Google Spain et Google, a notamment consacré le « droit à l'oubli » (en interprétant la directive 95/46/CE, susmentionnée). En principe, selon la Cour, l'exploitant d'un moteur de recherche sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers. Ceci peut notamment avoir pour conséquence que, lorsque, à la suite d'une recherche effectuée à partir du nom d'une personne, la liste des résultats inclut un lien vers une page web qui contient des informations sur la personne en cause, celle-ci peut s'adresser directement à l'exploitant du moteur de recherche ou, lorsque celui-ci ne donne pas suite à sa demande, saisir les autorités compétentes pour obtenir, sous certaines conditions, la suppression de ces résultats. La Cour a considéré, entre autres, qu'il était indispensable de trouver un équilibre entre, d'une part, le droit à l'oubli de la personne concernée, en particulier dans des situations où un certain laps de temps s'est écoulé depuis qu'une information concrète la concernant avait été publiée, et, d'autre part, l'intérêt légitime des internautes potentiellement intéressés à avoir accès à cette information. Selon la Cour, dans ce contexte, la recherche du juste équilibre devait être effectuée en tenant compte tant du droit au respect de la vie privée et du droit à la protection de données à caractère personnel. À cet égard, il a été relevé que, si, certes, les droits de la personne concernée prévalaient, en règle générale, sur les intérêts des internautes, cet équilibre pouvait, néanmoins, dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée, ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique.

Enfin, il peut être intéressant d'ajouter que, dans ce même arrêt, la Cour a pris position, notamment, sur le champ d'application territorial de la directive en cause, et ce en se basant sur le fait que Google Spain constituait une filiale de Google Inc., sur le territoire espagnol et, partant, un « établissement » au sens de celle-ci. La Cour a, en outre, rejeté l'argument selon lequel le traitement de données à caractère personnel par Google Search n'était pas effectué dans le cadre des activités de cet établissement en Espagne. La Cour considère à cet égard que, lorsque de telles données sont traitées pour les besoins d'un moteur de recherche exploité par une entreprise qui, bien que située dans un État tiers, dispose d'un établissement dans un État membre, le traitement est effectué « dans le cadre des activités » de cet établissement, au sens de la directive, dès lors que celui-ci est destiné à assurer, dans l'État membre en question, la promotion et la vente des espaces publicitaires proposés sur le moteur de recherche en vue de rentabiliser le service offert par ce dernier.

Par ailleurs, la Cour a confirmé qu'il s'agissait bien d'une « collecte » d'information, au sens de la directive, lorsque le moteur de recherche traitait, de manière automatisée, constante et systématique, des informations publiées sur Internet. Selon la Cour, notamment, ledit exploitant « enregistrait » et « organisait » ces données[20] dans le cadre de l'indexation. Ensuite, celles-ci étaient conservées sur ses serveurs et, le cas échéant, communiquées aux utilisateurs, en mettant à leur disposition, suite à l'analyse des mots-clés demandés, les listes de résultats. Dans l'ensemble, il s'agissait ainsi bien d'un traitement d'informations.

Cet arrêt, particulièrement novateur, a eu de multiples répercussions dans la pratique. Certaines procédures ont suivi au niveau national. Quant aux chiffres concrets des demandes à ce qu'une personne soit « oubliée », ils peuvent s'avérer assez élevés dans certains États, et plus bas dans d'autres. Partant, à titre d'exemple, alors qu'en France, État en tête des demandes, il s'agirait de plus d'un million de demande de déréférencement ayant été introduites auprès de Google, depuis mai 2014 [283 276 demandes ont été faites, concernant précisément 1 030 182 URL (Uniform Resource Locator/ adresse d'une ressource Internet). La firme américaine a accepté d'en déréférencer moins de la moitié, à savoir 41,3 %][21], en revanche, au Grand-Duché de Luxembourg, depuis mai 2014, seules 514 demandes d'effacer un lien concernant une personne concrète ont été déposées. Après avoir analysé ces requêtes, Google a accepté près de la moitié de ces requêtes (48 % des URL ont été conservées)[22]. Quand on rapporte ces requêtes au nombre d'habitants, l'Estonie est en tête, suivie du Lichtenstein et des Pays-Bas. Les sites les plus touchés par ces déréférencements sont les principaux réseaux sociaux, tels que Facebook, Twitter, Google+ ou encore YouTube. Sont également concernés les sites agrégeant des informations sur les personnes, comme ProfileEngine, Yasni, 192.com, mais aussi le site de rencontres Badoo.[23] Enfin, il est intéressant de noter que, selon cette même source, les raisons mentionnées en tant que base pour le déréférencement incluent, outre la protection de la vie privée en générale, celles de la protection de l'enfance ou des personnes agissant dans la vie publique. Dans certains cas, il s'agit même d'exclure des informations qui concernaient, par le passé, certaines activités d'ordre criminel. Cependant, il convient de souligner que de nouveaux problèmes se posent, en effet, certains moteurs de recherche ou sites internationaux d'échange d'information tracent des internautes même non-membres des réseaux en cause, afin de diffuser des informations à leur égard.[24]

[20] Après avoir procédé à leur « extraction »;

[21] *« Droit à l'oubli: la France en tête des demandes »*; Le Monde; 15 juillet 2015;http://www.lemonde.fr/pixels/article/2015/07/15/droit-a-l-oubli-la-france-en-tete-des-demandes_4684029_4408996.html

[22] « Un droit à l'oubli mitigé »; dans l'Essentiel; 27 novembre 2015; page 5;

[23] *« Droit à l'oubli: la France en tête des demandes »*; Le Monde; 15 juillet 2015; http://www.lemonde.fr/pixels/article/2015/07/15/droit-a-l-oubli-la-france-en-tete-des-demandes_4684029_4408996.html

[24] Voir, par exemple, pour la Belgique, http://www.lemonde.fr/pixels/article/2015/11/09/la-belgique-ordonne-a-facebook-de-cesser-de-tracer-les-internautes-non-membres_4806107_4408996.html

Conclusion

Ces quelques lignes ont pour but de mettre en évidence les difficultés qui se présentent de nos jours, dans un contexte particulièrement complexe, lorsque nous parlons de la protection des données à caractère personnel. Qu'il s'agisse de trouver un équilibre entre certains intérêts publics et privés ou, tout simplement, de fixer des limites quant à ce qui est encore permis, lors de la collecte d'information, il est certain que nous nous trouvons dans un domaine dans lequel des solutions nouvelles seront encore adoptées pour tenir compte, notamment, du progrès technique. Ce n'est très probablement pas la base législative applicable aujourd'hui qui nous permet d'évaluer ce qui sera ou non permis dans les années à venir. La juridiction évolue elle aussi, sur beaucoup d'aspect, de manière rapide. Quant au législateur, il se doit de modifier les normes pertinentes en fonction des diverses situations qui se présentent dans les sociétés contemporaines, la réaction devant toujours mettre un accent plus ou moins fort sur la sécurité ou, au contraire, sur les droits fondamentaux, tels que la protection de la vie privée ou des données personnelles. De même, le progrès technologique est tellement rapide qu'il nécessite, notamment dans une société numérique, d'agir de manière conséquente pour que le cadre normatif corresponde encore à la réalité technique. Le grand danger est que, pour des raisons liées soit à la recherche d'une sécurisation à 100 %, impossible à atteindre selon certains, soit en raison de l'impact de plus en plus important des nouvelles technologies, notamment dans le contexte numérique, dans la vie de chacun, les droits de l'homme soient bafoués. À cet égard, il convient toujours de rappeler que ce sont les fondements même de notre société européenne qui consistent à mettre en avant l'individu et ses droits, sans pour autant pencher vers un « droit de l'hommisme ».

SCHWARZ JURAJ

PROTECTION OF PERSONAL DATA IN THE EUROPEAN UNION

(Summary)

*Structure of this study***:**

1. Short historical overview.
2. The role of the Court of Justice of the European Union (CJEU) – Progress in personal data protection, improvements due to the CJEU's case-law.
3. Analysis of current difficulties in the protection of personal data."