Cultures & Conflits

76 (hiver 2009)
Fichage et listing

Alex Türk et Pierre Piazza

La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée

Entretien avec Alex TÜRK ; propos recueillis par Pierre PIAZZA

Avertissement
Le contenu de ce site relève de la législation française sur la propriété intellectuelle et est la propriété exclusive de l'éditeur.
Les œuvres figurant sur ce site peuvent être consultées et reproduites sur un support papier ou numérique sous réserve qu'elles soient strictement réservées à un usage soit personnel, soit scientifique ou pédagogique excluant toute exploitation commerciale. La reproduction devra obligatoirement mentionner l'éditeur, le nom de la revue, l'auteur et la référence du document.
Toute autre reproduction est interdite sauf accord préalable de l'éditeur, en dehors des cas prévus par la législation en vigueur en France.

revues.org

Revues.org est un portail de revues en sciences humaines et sociales développé par le Cléo, Centre pour l'édition électronique ouverte (CNRS, EHESS, UP, UAPV).

Référence électronique
Alex Türk et Pierre Piazza, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011, consulté le 06 janvier 2013. URL : http://conflits.revues.org/17806

Éditeur : Centre d'études sur les conflits
http://conflits.revues.org
http://www.revues.org

Document accessible en ligne sur : http://conflits.revues.org/17806
Ce document est le fac-similé de l'édition papier.
Creative Commons License

La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée

Entretien avec Alex TÜRK

Propos recueillis par Pierre PIAZZA

Alex TÜRK est président de la Commission nationale de l'informatique et des libertés (CNIL) et du « Groupe de l'article 29 » [1].

Pierre PIAZZA est maître de conférences en science politique à l'université de Cergy-Pontoise et membre du CARPO (université de Versailles-St-Quentin).

C&C : Selon vous, quelles sont les raisons qui expliquent actuellement l'amplification et l'accélération du processus de collecte, de circulation et d'échange de données personnelles à l'échelon transnational ?

Alex Türk : Ce développement massif des échanges d'information m'apparaît tout d'abord lié aux avancées du progrès technologique. En matière informatique, cette accélération se traduit par des capacités grandissantes de collecte et de stockage de données personnelles, elles-mêmes de plus en plus diverses (données biométriques ou génétiques, données de réservation, antécédents judiciaires, etc.). Elle se traduit également par une interopérabilité croissante des systèmes d'information ou des données qui y sont enregistrées, ce qui en facilite naturellement la circulation.

---

1 . Également appelé « G29 », ce groupe de travail sur la protection des données a été créé par l'article 29 de la directive 95/45/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données. Il se compose de représentants de chaque autorité nationale de protection des données, du Contrôleur européen à la protection des données et de la Commission européenne. Sorte de « CNIL des CNIL européennes », cet organe consultatif indépendant sur la protection des données et de la vie privée est notamment chargé d'émettre des avis sur les questions relatives à la protection des données en Europe. Depuis 2008, le président de la CNIL exerce également les fonctions de président du G29, et la CNIL participe donc grandement aux travaux de ce groupe. Cf. [http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm]

Une autre caractéristique du progrès technologique est que ses effets sont marqués par une propension à s'universaliser, à se globaliser. Dans le domaine du traitement informatique de données, cela se traduit, bien sûr, par le formidable essor des délocalisations de traitements et l'émergence, dans des pays jusqu'alors peu impliqués dans le traitement de l'information, d'activités de développement logiciel, de sous-traitance et de maintenance à distance. La maîtrise, par les Etats-Unis, des modes de traitement et d'organisation de l'information (systèmes d'exploitation, logiciels, outils de recherche, etc.), conduit également à multiplier les échanges de données à destination de ce pays.

En ce qui concerne en particulier le domaine de la sécurité, ce phénomène d'échanges croissants de données s'explique également par la nécessité indéniable de mettre en œuvre une coopération policière européenne et internationale efficace. En effet, en Europe comme ailleurs, les attentats du 11 septembre 2001 se sont traduits par un renforcement des mesures de sécurité intérieure et de maîtrise des flux migratoires. Pour faire face aux défis que représentent notamment la criminalité transnationale et le terrorisme, mais également l'immigration clandestine, il apparaît ainsi inévitable de partager des informations plus nombreuses entre autorités répressives, afin de coordonner les actions en ces matières. Cet impératif politique de prévention et de répression des infractions se traduit donc par une forte augmentation du volume et du flux de données échangées entre les autorités policières européennes et internationales.

Enfin, un facteur primordial à mes yeux de ce développement grandissant des échanges est d'ordre plus psychologique, et consiste en ce que j'ai appelé le « mirage du fichier remède miracle ». En effet, il semble que lorsque les autorités publiques sont confrontées à un problème, elles ont une propension naturelle à créer un nouveau fichier. Si les autorités de protection des données savent pertinemment que la création d'un fichier informatique ne règle pas tout, elles doivent se battre régulièrement contre la tendance à sacraliser le caractère supposé infaillible du traitement informatique de données. Cette tendance est visible, par exemple, dans certaines décisions de création de fichiers qui ne sont ensuite jamais mises en œuvre, aussi bien au niveau national qu'européen, ou dans la création de fichiers qui ne sont pas adaptés à l'objectif recherché. Le mythe du contrôle absolu par l'instrument informatique est bien à l'œuvre, et explique lui aussi l'accélération des processus de circulation de données.

C&C : Quels sont, à vos yeux, les principaux problèmes que soulève un tel processus ?

Alex Türk : Il est difficile de résumer en quelques phrases l'ensemble des problèmes soulevés par ce phénomène. Premièrement, il faut noter l'extrême

diversité, voire l'absence dans de nombreux pays, de lois de protection des données personnelles. En effet, de nombreux pays ne disposent pas aujourd'hui encore de lois « informatique et libertés ». A vrai dire, les Etats en disposant ne représentent même qu'une minorité, puisque moins de 80 pays à travers le monde se sont dotés d'une telle législation. A cet égard, dans le cadre de la francophonie, la CNIL s'est fortement impliquée pour aider certains pays (Sénégal, Burkina Faso, Maroc, etc.) à se doter de lois de protection des données et d'autorités chargées de les faire appliquer. Mais l'existence d'une telle législation ou d'une autorité de contrôle ne doit pas être le seul indicateur. Encore faut-il que ces dispositions puissent être effectivement appliquées, et que les autorités de protection des données en aient les moyens. Or, je le répète bien souvent, même en Europe en ce qui concerne le groupe dit de l'article 29, les moyens dont nous disposons sont parfois insuffisants pour mener à bien l'ensemble de nos missions. En France, un plan de rattrapage engagé voici cinq ans nous amène progressivement à une situation correcte, en termes de budget et d'effectif par exemple [2].

Au sein même des pays où le droit à la protection des données est établi, les conceptions de celle-ci peuvent apparaître réellement divergentes. En Europe, la conception anglo-saxonne est ainsi sensiblement différente de la conception dite continentale, comme l'avaient déjà montré les débats préalables à l'adoption de la directive 95/46/CE 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, et comme le montrent aujourd'hui encore les discussions relatives à la révision de cette directive. Les standards européens de protection des données apparaissent en outre de plus en plus concurrencés par les standards américains en particulier, qui se diffusent dans certains forums internationaux comme l'APEC (*Asia-Pacific Economic Cooperation*), alors que le mode de régulation du traitement de données qu'ils proposent diffère sensiblement de la tradition européenne [3].

En second lieu, le droit français et le droit européen de la protection des données sont, par essence, trop étroits parce qu'ils s'inscrivent dans le cadre de territoires et de champs de compétences ordonnés et balisés. Dès lors, les

2 . Ainsi, les services de la CNIL comptent aujourd'hui environ 130 employés, alors qu'ils n'étaient que 75 en 2004. Si nous ne disposons pas encore de toutes les ressources nécessaires au bon exercice de nos missions, force est donc de constater que la situation s'est nettement améliorée au cours de ces dernières années.

3 . Ces divergences, au sein de l'Europe ou entre l'Europe et les Etats-Unis, se révèlent notamment dans le mode de régulation du traitement de données mis en œuvre par les autorités compétentes. Le concept d'*accountability* par exemple, qui sous-tend la conception américaine de la protection des données, renvoie au principe d'autorégulation sectorielle caractéristique de cette conception, tandis que la tradition continentale du droit à la protection des données met plus volontiers en exergue la nécessité de textes législatifs et réglementaires applicables. Autre exemple : la tradition anglo-saxonne fait appel à une gestion des données personnelles fondée sur le risque, à l'inverse de la position européenne qui prône une application généraliste de ce droit fondamental.

instruments mis en place pour contrôler les flux transfrontières de données apparaissent à la fois bien dérisoires et peu compréhensibles. Il faut donc avoir le courage de reconnaître que nos règles de protection des données peuvent apparaître, en ce domaine, inadaptées et que, de la même façon que l'informatique est aujourd'hui par nature communicante et sans frontières, la protection des données ne peut se concevoir que dans une dimension mondiale. Ceci suppose assurément d'élaborer, sur le plan mondial et non plus seulement national ou européen, un instrument juridique nouveau. Surtout, il nous faut, en amont, réfléchir à une adaptation (et non à une remise en cause) de nos concepts de base pour assurer une meilleure compréhension de ceux-ci (comme la notion de donnée à caractère personnel, le concept de droit d'accès, etc.). Il nous faut enfin accroître le niveau d'information et de prise de conscience des personnes.

C&C : Quel rôle spécifique l'Europe joue-t-elle dans ce processus à travers notamment le VIS, SIS II ou encore le Traité de Prüm [4] *?*

Alex Türk : L'Europe joue incontestablement un rôle important dans ce processus, et c'est pourquoi il convient de se départir de cette idée selon laquelle elle serait en position de « suiveur » des Etats-Unis, subissant passivement les assauts répétés d'autorités américaines avides d'informations de plus en plus nombreuses. Certes, de telles tentatives existent, et la CNIL comme le G29 ont été les premiers à s'élever contre les demandes abusives des autorités américaines, s'agissant par exemple du transfert des données des passagers à destination des Etats-Unis (accords PNR [5]) ou de l'accès aux données bancaires européennes (« l'affaire SWIFT » [6]). La mise en œuvre du programme d'exemption de visa (*Visa Waiver Program* – VWP [7]) se traduit également par une pression accrue des autorités américaines à l'échange de données, particulièrement à l'égard des « nouveaux États membres » (République Tchèque,

4 . Le VIS (*Visa Information System*), le Système d'Information Schengen II et le Traité de Prüm constituent trois initiatives récentes prises au niveau européen au travers desquelles se manifeste une volonté politique d'accentuer la collecte, l'échange et l'exploitation de données biométriques à des fins d'identification de certaines catégories d'individus. Cf. notamment sur ce point Pierre Piazza, « L'europe biométrique contre les libertés ? », *Regards sur l'actualité*, n° 349, mars 2009, et Sylvia Preuss-Laussinotte, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », *Cultures & Conflits*, n° 74, été 2009.

5 . Cf. [http://www.cnil.fr/la-cnil/actu-cnil/article/article//le-nouvel-accord-europeetats-unis-sur-les-donnees-des-passagers-aeriens-est-au-detriment-des-cit/] et [http://www.cnil.fr/la-cnil/actu-cnil/article/article//accord-pnr-eu-usa-les-termes-du-compromis/]

6 . Pour une description détaillée de « l'affaire SWIFT » et des enjeux auxquels elle renvoie en matière de protection des données personnelles, cf. l'article d'Anthony Amicelle et de Gilles Favarel-Garrigues dans ce numéro.

7 . Ce programme, établi de manière temporaire en 1986 et rendu permanent en octobre 2000 par le *Visa Waiver Permanent Program Act*, permet aux ressortissants de certains Etats de bénéficier d'une exemption de visa pour un séjour touristique ou pour affaires d'une durée inférieure à 90 jours. A ce jour, 27 Etats participent au programme, dont une grande partie de pays européens. Parmi les nombreuses modifications relatives aux modalités du programme, la loi adoptée en 2002, *The Enhanced Security Border and Visa Entry Act*, a prévu en particulier l'obligation pour les Etats qui ont été désignés pour y participer, de délivrer des passeports incluant des éléments d'identification biométrique et conformes aux standards de

Hongrie, Lituanie, Slovaquie, etc.). Mais l'Europe ne reste pas sans réponse face à ces nouvelles demandes, tente de coordonner son action et montre ainsi qu'elle peut parfois résister aux pressions américaines. Pas suffisamment ...

En ce qui concerne les échanges de données intra-européens, l'Union européenne (UE) est elle-même, depuis plusieurs années, très active et donne de nombreuses impulsions politiques et juridiques afin de faciliter les échanges de données, en matière notamment d'immigration ou de coopération policière. A l'intérieur de sa zone de compétence, l'UE met ainsi en place un espace d'échange et de mutualisation des données sans précédent historique. Or, cet espace n'est pas sans soulever de nombreux problèmes en termes de protection des données, car la mise en place de ces coopérations ne s'accompagne pas toujours de règles de protection satisfaisantes.

En matière d'immigration notamment, du fait de la création de la zone Schengen de libre circulation des personnes, la coopération européenne donne lieu à la création de bases de données mutualisées ou mises en réseau, telles que le Système d'information sur les visas (*Visa Information System* – VIS) [8], le Système d'information Schengen (SIS) [9] – pour les informations qui concernent les étrangers – ou le système Eurodac [10]. Adopté en décembre 2009 par le Conseil européen, le nouveau programme pluriannuel déterminant les actions à entreprendre et l'agenda à suivre pour la période 2010-2014 dans le cadre de l'espace de liberté, de sécurité et de justice (ELSJ), dit « programme de Stockholm [11] », prévoit la création de nouvelles bases de données. Ainsi, les autorités européennes envisagent la mise en place d'un système d'enregistrement électronique des entrées et sorties du territoire européen, sur le modèle du programme US-VISIT [12] des Etats-Unis ou de ce que les autorités fran-

---

l'OACI. En août 2007, le Congrès américain a, en outre, autorisé le *Department of Homeland Security* (DHS) à réformer le VWP afin de renforcer les mesures de sécurité requises pour les pays participants et d'élargir les conditions d'éligibilité pour les pays qui souhaitent y participer.

8 . Cf. la décision du Conseil du 8 juin 2004 portant création du système d'information sur les visas (VIS) ; Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les Etats membres sur les visas de court séjour (règlement VIS) ; la Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des Etats membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière.

9 . Cf. notamment le Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

10 . Cf. le Règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.

11 . [http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf]

12 . Le programme US-VISIT est constitué par un ensemble de mesures de sécurité mises en place par le *US Department of Homeland Security* à la suite des attentats du 11 septembre 2001 afin de déterminer avec certitude l'identité des voyageurs pénétrant sur leur territoire des Etats-Unis (recours aux identifiants biométriques) et vérifier qu'ils n'y prolongent pas leur séjour au-delà de la période de validité fixée par leur visa.

çaises ont déjà mis en œuvre dans le cadre du fichier VISABIO [13]. Il est également proposé la création d'un système européen d'autorisation préalable de voyage, dit EU ESTA, de nouveau semblable au système mis en œuvre par les Etats-Unis. Ces enregistrements mutualisés portent en outre souvent sur des données particulièrement sensibles, et notamment des données biométriques.

En ce qui concerne la coopération policière et judiciaire européenne, les échanges se font également de plus en plus nombreux. Ils interviennent dans le cadre d'instruments juridiques particuliers, comme le traité de Prüm par exemple, dont certaines dispositions ont été intégrées dans le droit de l'UE en 2008, et qui permet notamment des échanges de données génétiques entre autorités répressives, mais également d'empreintes digitales ou d'immatriculation de véhicules. Le SIS constitue également un outil de coopération policière. Plusieurs textes européens, qui n'ont pas encore fait l'objet de transposition par tous les Etats membres, prévoient enfin de manière plus générale, des conditions d'échange de données très favorables à leur circulation, malgré le caractère sensible des données pouvant être échangées. Il en est ainsi des décisions-cadre du 18 décembre 2006 [14] et du 27 novembre 2008 [15] dont l'objet est de mettre en œuvre le principe de disponibilité des informations en matière répressive.

Dans l'ensemble, ces échanges de données apparaissent limités à la zone européenne : les transmissions d'information à des Etats tiers font l'objet de nombreuses restrictions dans l'ensemble des instruments mentionnés. Cependant, les autorités européennes adoptent un comportement similaire aux autorités américaines, en demandant de plus en plus d'informations à certains Etats tiers, dans un cadre bilatéral ou multilatéral. Les autorités nationales, françaises par exemple, mettent ainsi en place des mécanismes d'échanges de données avec de nombreux Etats, par le biais d'accords portant sur des domaines spécifiques (drogue, prostitution, terrorisme, immigration

13 . « Le nouveau traitement dénommé VISABIO généralise les expérimentations menées depuis 2004 par le ministère de l'intérieur et le ministère des affaires étrangères dans le cadre du programme BIODEV autorisé par le décret du 5 octobre 2004. Il s'agit désormais de collecter les données biométriques (photographie numérisée et empreintes digitales des dix doigts) de tous les demandeurs de visa et de les conserver dans deux bases centrales reliées par un lien chiffré, avec les données d'identité qui étaient déjà précédemment recueillies. Plus de deux millions d'étrangers ressortissants de pays soumis à l'obligation de visa seront concernés chaque année », Délibération de la CNIL n° 2007-195 du 10 juillet 2007 portant avis sur le projet de décret pris pour l'application de l'article L. 611-6 du code de l'entrée et du séjour des étrangers et du droit d'asile portant création d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa et modifiant la partie réglementaire de ce même code, [http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000825669&dateTexte]

14 . Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'UE.

15 . Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

clandestine, etc.). L'UE demande également à être rendue destinataire de plus nombreuses informations, en particulier en matière d'immigration et d'asile, de la part des pays d'origine et des pays de transit des migrants, afin de lutter plus efficacement contre l'immigration clandestine.

C&C : Dans le cadre d'un tel processus, les autorités de protection des données (la CNIL, le G29, le CEPD) vous semblent-elles complètement désarmées, en particulier dans les domaines qui relèvent du 3e pilier de l'UE ?

Alex Türk : Elles ne sont certes pas « complètement désarmées » mais ont véritablement de grandes difficultés à réguler ces échanges de données. A mes yeux, ces difficultés sont liées principalement à l'encadrement juridique insuffisant de ces échanges. En effet, sur le plan européen, mis à part les deux décisions-cadre précitées qui encadrent les échanges de données entre autorités répressives, et les dispositions spécifiques insérées dans des textes particuliers (comme dans le cadre de l'accès des autorités répressives au VIS, du prochain accès au système Eurodac, de Prüm, des centres de coopération policière et douanière frontaliers, etc.), il n'existe pas actuellement de cadre juridique permettant un niveau de protection des données satisfaisant s'agissant des traitements relevant du 3e pilier de l'UE. Rappelons en effet que la directive 95/46/CE ne « couvre » que les traités relevant du 1er pilier du droit européen.

C'est d'ailleurs pourquoi notre Commission ainsi que les autorités de protection des données européennes soutiennent les initiatives actuelles de réforme du régime de protection des données, qui apparaissent d'autant plus nécessaires dans la perspective de l'entrée en vigueur du traité de Lisbonne, dont certaines dispositions ont justement pour objet d'harmoniser le régime de protection des données à l'intérieur de l'UE, quel que soit son domaine d'application [16]. Il conviendrait donc que l'ensemble des traitements, y compris ceux ayant pour finalité la sécurité publique ou les activités relatives aux domaines du droit pénal, soient soumis aux mêmes règles de protection des données, même si certaines modalités spécifiques devront être prévues pour ces derniers. Enfin, les autorités de protection des données nationales ne pourront efficacement jouer leur rôle que si ces règles s'appliquent également aux traitements nationaux de police.

Cependant, les autorités de protection des données se sont progressivement armées pour tenter d'influer sur ce processus d'accélération des échanges de données. Ainsi, la plupart des structures européennes de coopération policière ou judiciaire sont dotées d'organes de supervision internationaux (les autorités de contrôle communes, ou AAC). C'est le cas du système Schengen, d'Europol, d'Eurojust, ainsi que du système d'information douanier. Par ail-

16 . Cf. l'article 16 du futur traité sur le fonctionnement de l'UE, l'article 6 du futur traité sur l'UE, ainsi que la déclaration n° 21 annexée à l'acte final de la conférence ayant adopté le traité de Lisbonne.

leurs, un « groupe de coordination », présidé par le Contrôleur européen de la protection des données (CEPD), est chargé de contrôler le fonctionnement du système Eurodac. Le CEPD assure également une mission de supervision des traitements de données à caractère personnel mis en œuvre par les agences et institutions européennes.

En outre, un groupe de travail sur la police et la justice (dit WPPJ pour *Working Party on Police and Justice* [17]) a été créé par la Conférence européenne des autorités de protection des données en 2007. Sur le modèle du G29, il rassemble les représentants des autorités nationales de protection des données et du CEPD, et a pour mission de suivre et d'examiner les initiatives européennes en matière de police et de sécurité. La création de ce groupe vise ainsi à compenser l'absence de compétence du G29 sur les politiques relevant du 3e pilier de l'UE, exclues du champ d'application de la directive 95/46/CE. Toutefois, ce groupe n'a aucune existence juridique et ne peut donc jouer qu'un rôle consultatif limité.

Par ailleurs, ces faiblesses ne concernent pas uniquement les matières relevant du 3e pilier de l'UE. Ainsi, les moyens financiers du G29 apparaissent toujours insuffisants, et son fonctionnement est tributaire de la Commission européenne dont l'unité « protection des données » de la Direction générale Justice, Liberté, Sécurité (DG JLS) en assure le secrétariat. En outre, le G29 ne dispose d'aucun pouvoir de sanction, alors que celui-ci constitue à mon sens une prérogative nécessaire à l'application effective du droit à la protection des données des personnes.

C&C : Les autorités de contrôle communes (Europol, Schengen et Système d'information douanier) et organe de contrôle commun (Eurojust) vous paraissent-ils mener une action efficace en matière de protection des données personnelles ?

Alex Türk : En dépit de moyens budgétaires limités et de pouvoirs variant en fonction des différents cadres juridiques, les ACC ont la possibilité de mener des contrôles sur place et doivent être consultées pour avis sur les nouveaux traitements ou nouveaux développements mis en œuvre au sein de chacune de ces structures.

Elles ont également pour fonction d'harmoniser les activités respectives des autorités nationales de contrôle. Cette activité peut être tout à fait déterminante dans le cadre de l'exercice par les personnes de leurs droits d'accès, de rectification et de suppression des données qui les concernent, car les mutualisations ou échanges de données rendent souvent cet exercice difficile. L'ACC Schengen par exemple, par ses travaux, tente ainsi d'éviter et de régler les

17 . [http://www.privacycommission.be/fr/static/pdf/working-party-on-police-and-justice-ar-fr.pdf]

interprétations divergentes de la Convention d'application des accords de Schengen qui peuvent naître entre les autorités de contrôle, afin d'harmoniser sur le territoire européen les conditions d'exercice de ces droits fondamentaux.

Enfin, les ACC publient régulièrement leurs rapports d'activité, contribuant ainsi à renforcer les prises de conscience, tant des autorités que des personnes, des problèmes concrets causés par la multiplication des bases de données en Europe.

Certaines ACC ont des pouvoirs plus importants : l'ACC Europol, par exemple, dispose de son propre site web, sur lequel elle communique et diffuse des informations quant à son activité, mais aussi informe les citoyens de leurs droits. Les demandes d'exercice de leur droit d'accès par les citoyens auprès d'Europol ont ainsi fortement augmenté à la suite de ces campagnes de sensibilisation, ce qui démontre que certaines des actions des ACC peuvent être efficaces. En outre, l'ACC Europol procède à des inspections annuelles. Elle intervient également dans les procédures de négociation d'accords de coopération entre Europol et des Etats tiers. Dernièrement, elle a ainsi joué un rôle non négligeable dans le refus adressé à la Russie d'ouvrir de telles négociations, considérant que cet Etat n'avait pas un niveau de protection des données suffisant.

Le « groupe de coordination Eurodac » fournit un autre exemple de l'utilité réelle de ces instances de supervision. Dans le cadre de son second rapport d'inspection de la base de données européenne, ce groupe a émis des recommandations visant notamment à améliorer les modalités d'information des demandeurs d'asile, qui ont partiellement été reprises dans le récent « paquet législatif » proposé par la Commission européenne afin de modifier le système Eurodac [18].

Ainsi, la vigilance des ACC, leur collaboration étroite avec les délégués à la protection des données internes aux organismes concernés et la participation active des représentants des autorités nationales de protection des données, permettent d'obtenir des résultats tangibles. Cependant, il est clair que leur rôle et leurs moyens d'action sont encore insuffisants, que leur mode de fonctionnement pourrait être largement amélioré, et que l'exercice effectif des droits des personnes à la protection des données ne pourra être atteint par le seul recours à ces dispositifs.

C&C : Reposant sur de nouveaux principes (disponibilité de l'information, interopérabilité des systèmes, etc.) et l'exploitation de nouvelles formes de données (biométrie, PNR, etc.), ce processus de collecte, de circulation et d'échange

18 . Cf. notamment les documents COM (2009) 342, 343 et 344 du 10 septembre 2009.

de données personnelles à l'échelon transnational ne vous semble-t-il pas symptomatique de la mise en oeuvre de formes inédites de contrôle ou de surveillance des individus ?

Alex Türk : On peut en effet estimer que ce processus a contribué d'une certaine façon à augmenter le niveau de contrôle et de surveillance opéré sur les citoyens. Mais il faut, je crois, bien comprendre le contexte. C'est ce que j'appelle la « vague sécuritaire », qui a déclenché, depuis les attentats du 11 septembre et les autres attentats terroristes survenus par la suite, un mouvement profond, qui se comprend parfaitement, tant de la part des autorités étatiques que de l'opinion publique, en faveur d'un renforcement des moyens d'action en matière de lutte contre le terrorisme ou la criminalité.

Cette vague sécuritaire est tout d'abord normative : elle se traduit par la création ou l'extension de nombreux fichiers et la mise en place, au profit des autorités de police, de nouveaux moyens d'investigation dans les systèmes d'information. Faire ce constat ne revient pas à contester le bien-fondé même de ces politiques, qui semblent répondre aux attentes de nos concitoyens. Les autorités de contrôle se situent en effet en dehors du champ politique et ne se confondent ni avec des associations militantes, ni avec les autorités publiques en charge de la sécurité ou de la justice. Leur rôle est d'examiner les textes qui leur sont soumis, en recourant aux principes et aux instruments que les textes fondateurs du droit à la protection des données leur ont confiés (appréciation de la finalité et de l'adéquation entre cet objectif et les moyens mis en œuvre, évaluation des garanties de confidentialité et du respect des droits des personnes, etc.). Face à cette vague sécuritaire, les autorités de protection des données doivent ainsi éclairer les réflexions des citoyens et des autorités publiques afin de leur permettre de mesurer à quelles limitations de leurs droits individuels la société est prête à consentir pour accroître son niveau de sécurité collective et individuelle. C'est donc ce que nous tentons de faire dans nos activités quotidiennes, conscients du degré de responsabilité qui nous incombe.

Cette vague sécuritaire est également technologique, comme vous le mentionnez très justement. Plus généralement, ces nouvelles formes de surveillance reposent sur cette croyance que j'ai abordée plus haut, ce mythe du contrôle absolu par l'instrument informatique. Cette croyance est chaque jour alimentée par le développement technologique des systèmes d'information, toujours plus performants. Dans ce contexte, il est indispensable, du point de vue éthique comme du point de vue juridique, de continuer à affirmer que l'informatique peut être faillible, et donc de proscrire la prise de décision automatique par ordinateur, tout particulièrement dans des domaines tels que la sécurité ou la justice. Il s'agit là d'un combat difficile, dans la mesure où cette tendance à automatiser les modalités de contrôle des individus prend de l'am-

pleur. L'exemple de la biométrie est sur ce point révélateur : considérée comme la panacée en matière d'identification et d'authentification, alors même qu'elle n'a jamais fait l'objet d'une évaluation officielle, concertée sur le plan international, la biométrie se développe aujourd'hui massivement, et prend une part de plus en plus importante dans les processus d'identification administrative, sans qu'aucune réflexion réelle n'ait été conduite sur les conséquences à l'égard des personnes des erreurs d'identification biométrique. On le voit, le développement de nouvelles formes de contrôle nécessite au préalable une réflexion de fond et une évaluation à la fois de la mesure et de la technique utilisée.

A mon sens, ces considérations justifient d'autant plus l'existence et les missions dévolues aux autorités de protection des données. Celles-ci doivent à la fois procéder à un examen minutieux de l'ensemble des mesures pratiques de mise en œuvre de nouveaux traitements, de nouvelles modalités de collecte ou encore de nouvelles catégories de données personnelles. Elles doivent également être mises en capacité, par les pouvoirs publics, d'exercer efficacement leurs missions, c'est-à-dire d'avoir des moyens tant juridiques que budgétaires suffisants.

C&C : Ne bascule-t-on pas de plus en plus d'une logique d'authentification/identification vers une logique de traçabilité et de profilage des individus ? Ce phénomène fait-il naître chez vous de nouvelles craintes ? Selon vous, renvoie-t-il à des formes originales de « gouvernance » impliquant une redéfinition des rôles entre acteurs publics et privés en matière de sécurité ?

Alex Türk : Le développement des techniques de profilage est indéniable et soulève d'importantes difficultés de principe et de positionnement du curseur. Il semble encore trop tôt pour qualifier ce développement de passage d'une logique à une autre, ces fonctions d'identification et de traçabilité ne me paraissant pas exclusives l'une de l'autre, mais bien plutôt combinées dans les dispositifs de contrôle et de surveillance des individus.

En Europe, pour le moment, le profilage reste encore largement monopolisé par le secteur privé. Mais les autorités publiques commencent à investir ces techniques, comme le montre notamment le projet dit « PNR Europe » en cours d'élaboration [19]. Ce projet permettra aux autorités répressives de déterminer le degré de « dangerosité » des passagers aériens à destination ou en provenance d'un Etat européen en fonction d'informations diverses relatives à leur état civil, aux destinations, à la fréquence et à l'ensemble des détails de

19 . Il s'agit, à des fins de lutte contre le terrorisme et la criminalité organisée, d'imposer aux transporteurs aériens dont les vols sont à destination de l'Union européenne de communiquer par voie électronique aux institutions répressives des Etats membres des données relatives aux passagers ; [http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=COMfinal&an_doc=2007&nu_doc=654]

leurs trajets aériens, et d'autres informations puisées dans les différentes bases de données nationales ou européennes. En fonction de l'indicateur de risque ainsi élaboré, les autorités compétentes procèderaient ensuite à des contrôles, physiques ou d'enquête, plus poussés sur les individus repérés. Les profils élaborés permettraient également, selon les autorités, de repérer et de réprimer de nouvelles « techniques » criminelles (réseaux de trafiquants de drogue, circuits de prostitution, trajectoires terroristes, etc.).

Cette initiative européenne peut en effet légitimement susciter des inquiétudes. Elle confirme tout d'abord cette tendance à utiliser de nouvelles techniques, à créer de nouveaux fichiers, avant même qu'une définition précise des besoins et qu'une évaluation de l'utilité d'un tel traitement ou des carences des outils déjà mis en œuvre n'aient été rigoureusement effectuées. En effet, l'utilité de l'exploitation des données PNR par les autorités américaines s'agissant de la lutte contre le terrorisme n'est à ce jour pas clairement démontrée, et la CNIL ne dispose d'aucune donnée statistique sur ce point. Des études récentes et détaillées [20] concluent d'ailleurs à la prudence s'agissant de l'utilité des outils de *datamining* en matière de lutte contre le terrorisme ou la criminalité transnationale, et soulignent les risques de « faux positifs », c'est-à-dire d'identification de personnes innocentes comme étant suspectes.

Le recours au *profiling* par les autorités policières fait également naître des risques de violation du principe fondamental de non-discrimination, qu'a très justement soulignés l'Agence des droits fondamentaux de l'UE [21]. En effet, on voit bien le risque que ces profilages soient partiellement basés sur des généralisations stéréotypées concernant l'appartenance ethnique, religieuse ou la nationalité des personnes, surtout en matière de lutte antiterroriste. L'interdiction du profilage discriminatoire, qui semble actée dans le cadre du PNR Europe, appelle en outre des garanties procédurales, d'autant plus nécessaires s'agissant de mesures de surveillance secrètes, car le secret comporte un plus grand danger d'abus. Dès lors, le développement de ces techniques implique le contrôle par des autorités indépendantes des traitements mis en œuvre. Mais les autorités de protection des données sont-elles aujourd'hui en capacité de contrôler efficacement des bases de données si volumineuses ?

De manière plus générale, ce projet de PNR Europe est révélateur du phé-

20 . Cf. par exemple : Fred H. Cate, "Government Data Mining, the Need for a Legal Framework", *Harvard Civil Rights - Civil liberties Law Review*, vol. 43, n° 2, 2008) ; Jeff Jonas et Jim Harper, "Effective counterterrorism and the limited role of predictive data mining", *Policy analysis*, n° 584, 11 décembre 2006 ; et *Protecting individual privacy in the struggle against terrorists : A framework for program assessment*, un rapport (en date du 7 octobre 2008) de l'Académie nationale des sciences des Etats-unis d'Amérique, financé par le *Department of Homeland Security* (DHS).

21 . Cf. Agence des droits fondamentaux de l'UE (FRA), « *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes* », 28 octobre 2008.

nomène de l'utilisation croissante des données privées par les autorités répressives. Les autorités de protection des données ont déjà eu l'occasion de souligner à plusieurs reprises les dangers liés à cette double utilisation de données commerciales, dans le cadre des accords PNR signés en premier lieu avec les Etats-Unis dès 2004 et qui tendent aujourd'hui à se généraliser à travers le monde, mais également dans le cadre de la directive européenne relative aux services de communications électroniques, qui oblige les fournisseurs à conserver les données de connexion en vue de garantir la disponibilité de ces données à des fins policières [22]. Au niveau national, la même tendance peut être observée, dans les dispositions de la loi anti-terroriste par exemple [23]. Si l'objectif d'assurer la sécurité des personnes ne saurait être contesté par les autorités de protection des données, il est en revanche de leur devoir de rechercher en permanence, au nom de la société, un équilibre entre ces impératifs de sécurité publique et les exigences de la protection de la vie privée. Or, cette utilisation de données commerciales constitue indéniablement une entorse au principe fondamental de finalité selon lequel l'objectif d'un traitement doit être défini de façon précise et explicite, afin d'être en mesure d'apprécier si les moyens mis en œuvre sont proportionnés à ces objectifs. Si, dans le cadre des enquêtes judiciaires, il apparaît totalement légitime que les autorités publiques aient accès à toute information utile à la manifestation de la vérité, il est différent de postuler *a priori* que toute donnée personnelle peut être utilisée par les autorités policières avant la commission d'infractions, ou même avant qu'un soupçon étayé pèse sur telle ou telle personne.

Ces nouveaux dispositifs semblent, dès lors, appelés à se développer massivement à l'avenir, car quelle limite pourrait être appliquée à ce phénomène ? Comment décider que les données de réservation aérienne puissent être ainsi accessibles *a priori* aux autorités policières, mais pas les données téléphoniques, les données de connexion Internet, les données clients des entreprises, etc. ? On le voit, les possibilités sont infinies, et les propriétés du progrès technologique, et en particulier son caractère irréversible, rendent tout retour en arrière bien peu probable. C'est pourquoi cette tendance à l'utilisation de données privées à des fins de prévention d'infractions me paraît très inquiétante. On ne saurait en effet prévoir précisément les effets sociaux de ces dispositifs ou leurs conséquences en termes de contrôle des données personnelles par les citoyens ou par les autorités de protection des données. Il existe un risque que ces éléments s'ajoutent à d'autres, se conjuguent, se combinent, créent des synergies et aboutissent finalement à des situations échappant à tout contrôle personnel ou démocratique.

---

22 . Cf. la Directive 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 2002/58/CE.

23 . Loi n° 2006-64 du 23 janvier 2006 modifiée relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Dans ces conditions, quels sont les moyens d'action des autorités de protection des données ? Il convient en premier lieu de prendre la mesure du phénomène et de proposer des encadrements juridiques précis et efficaces. A cet égard, notre Commission participe activement aux travaux en cours au sein du Conseil de l'Europe [24] visant à définir juridiquement le profilage et à lui appliquer des règles de protection des données spécifiques. En outre, dans le cadre du PNR Europe par exemple, le G29 et le CEPD tentent d'introduire une clause de caducité du système qui permettrait, après un certain délai de mise en œuvre et une évaluation approfondie de l'utilité des mesures prévues prenant en compte leur impact sur les droits fondamentaux des citoyens, d'avoir un débat de fond avant toute pérennisation du système. Il convient également de réaffirmer la primauté du contrôle humain sur le contrôle informatique, en particulier en matière de sécurité publique : comme le rappellent la directive 95/46/CE d'octobre 1995 et la loi française « informatique et libertés » de janvier 1978, aucune décision de justice ou décision produisant des effets juridiques ne peut avoir pour fondement un traitement de données destiné à définir le profil d'un individu ou à évaluer certains aspects de sa personnalité. Enfin, il faut que les autorités de protection des données puissent jouer pleinement leurs rôles de conseil des autorités publiques et d'information des citoyens.

C&C : Ce processus de collecte, de circulation et d'échange de données personnelles à l'échelon transnational génère-t-il de nombreux dysfonctionnements, erreurs, négligences, etc. dont les individus sont amenés à pâtir ? Dans le cadre de ce processus, avez-vous des exemples précis relevant de tracasseries d'ordre bureaucratique ou de pratiques discriminatoires subies, de difficultés éprouvées afin de ne plus être répertorié dans certains fichiers à la suite d'inscriptions indues, de situations engendrant une privation de droits et de ressources, etc. ?

Alex Türk : Par essence, la multiplication des listes, des fichiers, des interconnexions, des transferts de données augmente évidemment les risques d'erreurs ou de dysfonctionnements, parfois au détriment de citoyens totalement innocents, mais également au détriment de l'efficacité des systèmes mis en œuvre, ce qui peut avoir de graves conséquences dans le cadre des traitements intéressant la sécurité publique.

L'exemple des données biométriques est à cet égard significatif. Notre Commission ne cesse de rappeler que ces identifiants, et notamment les empreintes digitales, présentent des risques particuliers au regard de la protection des données personnelles et des libertés, dans la mesure où ils permettent

24 . Le bureau du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe travaille actuellement à un projet de recommandation sur la protection des données traitées dans le cadre du profilage.

à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir. Les données biométriques peuvent être en outre capturées et utilisées à l'insu des personnes concernées, notamment à des fins d'identification policière ou d'usurpation d'identité. En outre, elles ne constituent pas un identifiant infaillible, car toute comparaison biométrique constitue une opération mathématique reposant sur l'évaluation de probabilités, et comporte donc des risques de fausses acceptations et de faux rejets. En outre, la collecte de ces identifiants n'est pas toujours physiquement possible, ni exploitable, par exemple dans les cas de personnes privées de mains ou de doigts ou encore d'empreintes abîmées par l'utilisation de produits corrosifs. Ces impossibilités sont généralement évaluées à environ 3 % de la population concernée par un dispositif, ce qui, pour des systèmes à grande échelle, peut comprendre un nombre très important de personnes.

Ainsi, la CNIL est témoin d'un nombre important de « tracasseries » administratives liées à ces problèmes de collecte ou d'enregistrement des empreintes digitales. La mise en place durant l'été du dispositif des passeports biométriques a, par exemple, donné lieu à de nombreux retards dans la délivrance des passeports, occasionnant pour certains de nos concitoyens l'annulation de leurs vacances et des frais financiers correspondants. Récemment, une personne atteinte d'un cancer voyageant aux Etats-Unis a ainsi été bloquée plusieurs heures à la douane américaine, car ses empreintes digitales avaient été effacées sous l'effet d'un médicament utilisé pour le traitement de sa maladie. De manière plus significative, de nombreux témoignages révèlent que certains demandeurs d'asile ou immigrés clandestins, dont les empreintes digitales peuvent être enregistrées dans le système Eurodac, pratiquent l'automutilation afin d'effacer leurs empreintes, se brûlant au fer rouge ou utilisant du papier de verre, pour échapper au fichage européen qui les empêcherait d'atteindre leur pays de destination. Ces témoignages doivent appeler l'attention des autorités sur les effets pervers de l'utilisation des technologies biométriques, et plus globalement sur la nécessité de procéder à une réflexion réelle et profonde sur les changements sociaux que cette utilisation peut provoquer.

Les problèmes de mise à jour des fichiers publics donnent également lieu à de nombreuses difficultés pour certains de nos concitoyens. Des problèmes d'homonymie par exemple, peuvent occasionner des contrôles poussés aux frontières pour certaines personnes qui portent un nom signalé dans le SIS. De même, certains étrangers sont régulièrement importunés à leur passage aux frontières du fait d'une incomplète mise à jour du fichier des personnes recherchées (FPR) : les personnes ayant fait l'objet d'un arrêté de reconduite à la frontière annulé ou abrogé restent quand même inscrites dans le fichier, en raison de l'absence de transmission d'informations vers le système central. Sur une plus grande échelle, notre Commission appelle régulièrement l'attention

des autorités sur les nombreux dysfonctionnements du STIC [25], dont l'utilisation dans le cadre d'enquêtes administratives donne parfois lieu à des pertes d'emploi ou des refus d'embauche indus.

Les transferts internationaux de données provoquent également des situations individuelles difficiles. En premier lieu, ces transferts constituent un réel obstacle à l'exercice des droits des personnes à l'accès ou à la rectification des données qui les concernent, car il est difficile de savoir qui détient ces données, qui est responsable de leur enregistrement ou de leur mise à jour. Nos autorités de protection des données sont là pour les aider à exercer ces droits, mais elles-mêmes sont parfois dans l'incapacité de retracer les évènements et d'identifier les responsables, ou se heurtent à des contradictions juridiques.

En outre, les autorités de protection sont confrontées à des transferts de données manifestement illégaux, sur lesquels il est donc très difficile d'exercer un contrôle, malgré les problèmes que ces transferts occasionnent pour les personnes qui y sont confrontées. Ainsi, très récemment, les autorités américaines ont-elles exigé que les 200 personnes d'un vol Air France Paris-Mexico survolant le territoire américain soient déroutées vers la Martinique, en raison de la présence à bord d'une personne figurant sur une liste d'interdits de vol (*no-fly lists*). Cet épisode s'est renouvelé une seconde fois, sur le même trajet, alors que la personne concernée était manifestement inscrite en toute illégitimité sur la *no-fly list* américaine. En tout état de cause, la transmission de telles informations, rendue obligatoire par la loi mexicaine, aurait dû être notifiée à notre Commission qui aurait alors pu vérifier que les exigences de protection des données étaient respectées. La transmission de ces mêmes informations vers les Etats-Unis constitue une autre dérogation préoccupante à notre droit national.

Pointer ces dysfonctionnements, ces erreurs, ces transgressions du droit et les nombreux problèmes pratiques qu'ils occasionnent pour les personnes dont les données sont collectées, enregistrées et échangées, constitue précisément une des missions de notre Commission et de l'ensemble des autorités de protection des données. Ces actions sont parfois suivies d'effets, et notre Commission parvient ainsi à dénouer nombre de ces situations. Il est cependant dommageable que nos discours et nos actions ne soient pas davantage pris en compte par les autorités, qui doivent, je le répète, s'interroger et interroger la société civile, sur les conséquences du fichage à grande échelle des individus.

25 . Le Système de traitement des infractions constatées (STIC) répertorie des informations provenant des comptes-rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées. En décembre 2008, le STIC recensait 5 552 313 individus mis en cause. Pour un compte-rendu détaillé des nombreux problèmes affectant le fonctionnement de ce fichier, voir les résultats des contrôles effectués par la CNIL en 2008, disponibles sur notre site Internet : [http://www.cnil.fr/]

C&C : Que préconisez-vous comme solutions pour protéger plus efficacement les individus affectés par de telles situations induites par la collecte, la circulation et l'échange de données personnelles à l'échelon transnational ?

Alex Türk : Comme je l'ai déjà précisé, la première condition à mettre en œuvre afin de faire face à l'ensemble de ces processus est d'adapter le régime juridique général relatif à la protection des données. Si celui-ci apparaît, à certains égards, inadapté aux transformations actuelles du traitement informatique des données, ses principes doivent être réaffirmés et de nouveaux moyens efficaces de contrôle doivent être mis en œuvre afin de les faire appliquer.

Cette refonte passe notamment par l'élaboration d'un instrument juridique international et contraignant qui permette de combler les lacunes des outils actuellement en vigueur. Cet instrument devrait en premier lieu consacrer un droit universel à la protection des données et à la vie privée. Mais pour ce faire, il faut au préalable travailler à une harmonisation des conceptions mêmes de cette protection à travers le monde. Il faut également réfléchir aux meilleurs moyens permettant de déterminer les régimes juridiques applicables, afin notamment de faire face au défi que représentent à cet égard les échanges croissants de données, en Europe et au niveau international. Il faut en effet en finir avec cette fragmentation accrue du régime juridique de protection des données, y compris au niveau européen, qui rend nos droits illisibles et les droits des personnes complexes à exercer. Il faut enfin que cette lourde entreprise aboutisse à une élévation réelle du niveau de protection des données, à la mise en œuvre de garanties efficaces pour les citoyens, et que ces négociations internationales ne se traduisent pas, comme trop souvent, par un résultat correspondant au plus petit dénominateur commun.

En outre, la mondialisation des échanges et traitements de données induit un impératif de coordination accrue des méthodes d'action des différentes autorités de protection des données. C'est ce que j'ai proposé notamment lors de la conférence internationale des commissaires à la protection des données de Londres en novembre 2006 [26], durant laquelle j'ai appelé notre communauté à trouver un second souffle. En effet, nous sommes dans ce contexte sommés de développer fortement nos capacités d'expertise et de prospective, et pas uniquement sur le plan juridique. La protection des données pâtit aujourd'hui encore de son image trop juridique, alors que la crédibilité de nos institutions apparaît de plus en plus liée à notre capacité à comprendre et à anticiper les développements technologiques. C'est d'ailleurs la voie dans laquelle j'ai engagé la CNIL qui développe grandement, depuis plusieurs années, sa capacité d'expertise technologique, cas unique en Europe et dans le monde.

26 . [http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Londres-7112006-communiquer.pdf]

Or, ces capacités seront décuplées si les autorités de protection des données mettent en place des structures de coordination plus resserrées, mais aussi plus souples et plus réactives, voire proactives. Il nous faut mettre en commun notre savoir technologique et juridique, élaborer des stratégies de division du travail entre les autorités en fonction de leurs expériences, de leurs responsabilités, de leurs moyens. Il est également nécessaire de réfléchir aux relations que nous souhaitons et devons entretenir avec la communauté des chercheurs et les industriels des technologies de l'information et de la communication. Il faut aussi pallier l'extrême diversité de nos missions, de nos principes et moyens d'actions, de nos pouvoirs, etc. Face à la libre circulation de quantités illimitées d'informations entre des acteurs situés en tous points de la planète, il nous faut donc harmoniser nos actions.

Enfin, une priorité fondamentale dans ce contexte de libre circulation des données, me paraît être la prise de conscience par les citoyens des dangers et des risques auxquels ils sont confrontés, ainsi que des droits dont ils disposent à l'égard de leurs propres données. Les autorités de protection des données ont là encore une responsabilité majeure, qui pourrait se résumer ainsi : il faut communiquer. Il s'agit là d'un objectif prioritaire à mes yeux, car le droit à la protection des données est un droit fondamental et imprescriptible, dont la majorité de nos concitoyens n'a que très peu conscience. Il faut donc engager des actions pédagogiques puissantes, visant à les informer de l'existence et du contenu de ces droits, et à créer le « réflexe de la protection des données personnelles », ainsi que des mesures d'information mises en œuvre au sujet des fichiers existants. Cette stratégie de communication doit également s'exercer à destination des pouvoirs publics et des acteurs privés qui mettent en œuvre ces traitements de données, afin de les sensibiliser davantage à ces problématiques, de les engager à une réflexion profonde sur les conséquences de leurs initiatives.

Toutes ces actions apparaissent nécessaires pour parvenir à une meilleure reconnaissance institutionnelle et à une existence internationale plus forte, préalables à cette refonte du régime général de protection des données que j'appelle de mes vœux.

C&C : Votre idée d'organiser un « Kyoto des données personnelles » apparaît comme un début de réponse, mais n'apparaît-elle pas utopique au regard de l'extrême diversité (ou de l'absence) des autorités et des règles de protection des données à travers le monde ?

Alex Türk : Lors de la conférence internationale des commissaires à la protection des données et à la vie privée de Londres en 2006, j'ai en effet présenté, au nom de notre Commission, une initiative soutenue par les 75 délégations présentes. J'en ai déjà exposé les principaux éléments dans cet entretien, je n'y reviendrai donc pas en détail. Mais cette idée d'un « Kyoto des données

personnelles » m'apparaît pertinente et nécessaire pour atteindre cet objectif de renforcement, d'institutionnalisation et de stabilisation du droit à la protection des données personnelles.

En effet, chaque homme, et l'humanité dans son ensemble, est à la fois détenteur et responsable d'un capital. Et de même qu'on ne peut pas agir impunément en matière de protection de l'environnement, nous devons être extrêmement vigilants dans notre domaine, à l'égard de toute avancée technologique non maîtrisée comme de toute mise en œuvre de normes nouvelles consenties plus ou moins consciemment, parce que ce capital de garantie de nos libertés et de notre identité peut alors être amputé ou menacé dans son existence même. Or, la combinaison de ce que j'ai appelé les « vagues normative et technologique », qui vise à répondre aux exigences de sécurité collective de nos concitoyens par des outils informatiques toujours plus divers (biométrie, géo-localisation, vidéosurveillance, Internet, etc.), implique aujourd'hui des risques immenses pesant sur ces libertés et cette identité. Ce capital est ainsi chaque jour menacé et il y a donc urgence à le préserver, car, comme le capital environnemental de l'humanité, il risque, lui aussi, d'être si gravement atteint qu'il ne puisse être renouvelé.

C'est la lourde tâche qui incombe, notamment, à notre Commission et à l'ensemble des autorités de protection des données. De nombreux obstacles se dressent devant nous, que j'ai déjà mentionnés pour la plupart. En somme, il s'agit de prendre au sérieux le principe fondateur des lois « informatique et libertés », qu'exprime si brillamment l'article 1er de notre propre loi : « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Comme on le voit, le législateur, lui aussi, peut parfois succomber à la tentation de l'utopie !