



Les nouveaux moyens techniques de surveillance et  
la protection des droits fondamentaux –  
Défis pour les autorités judiciaires européennes

Vienne, le 10 juin 2009  
Justizpalast/Palais de justice

**Restrictions légales – Surveillance et droits fondamentaux**

Giovanni Buttarelli

Contrôleur européen adjoint de la protection des données

## *Introduction*

Cette conférence intervient immédiatement après un événement majeur sur le plan européen: la semaine dernière, la Commission européenne a publié une importante communication au Parlement européen et au Conseil intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens» (communication de Stockholm). Il s'agit de trois valeurs essentielles qu'il convient de renforcer dans une Europe fondée sur l'État de droit et les traditions constitutionnelles des États membres.

L'objectif déclaré de cette communication de Stockholm est de conférer une place centrale aux citoyens et à leurs droits (point 2.1). La communication affirme que *«dans l'espace de liberté, de sécurité et de justice, le respect de la personne et de la dignité humaine, énoncé dans la Charte, constitue une valeur essentielle. Les citoyens peuvent circuler librement et jouir pleinement de leurs droits dans cet espace sans frontières internes»*.

Concilier ces valeurs n'est cependant pas chose aisée.

Nous sommes entrés dans l'ère numérique et, dans ce domaine, le développement de nouvelles technologies profondément innovantes est intense et constant et la surveillance, qu'il convient d'entendre dans un sens moderne (dépassant la simple utilisation de caméras vidéo), joue un rôle croissant.

Nos pays présentent de plus en plus les nouvelles caractéristiques d'une société de la surveillance, caractérisée par une surveillance considérable de notre vie quotidienne à des fins diverses, parfois floues.

Permettez-moi de vous livrer ici quelques réflexions sur les demandes et attentes croissantes des services répressifs concernant l'utilisation des données à caractère personnel, les possibilités accrues d'utilisation des informations, l'impact de certains développements technologiques et la

nécessité qui en résulte de concevoir des moyens modernes et efficaces de protection des personnes.

### *Les besoins croissants d'utilisation d'informations*

Nous référant à nouveau au niveau européen, nous constatons que le programme législatif de l'UE de ces dernières années a été dominé par des initiatives portant sur l'adoption de nouveaux actes législatifs concernant l'information.

Je pourrais citer des dizaines de propositions et actes adoptés visant à faciliter le stockage, l'accès à et l'échange d'informations en vue de lutter contre la criminalité et le terrorisme, de contrôler efficacement les frontières extérieures de l'Union européenne mais aussi, plus généralement, de garantir la sécurité.

Plusieurs de ces actes sont bien connus. Dans cette liste impressionnante, citons:

- la directive de 2006 sur la conservation des données, qui impose la conservation des données relatives aux communications de tous les citoyens européens;
- la décision du Conseil concernant le traité de Prüm et la décision relative à sa mise en œuvre, qui imposent le stockage et l'échange des données ADN et dactyloscopiques entre les autorités des États membres;
- les nouveaux cadres juridiques applicables à Europol et Eurojust, qui aménagent pour ces organes des possibilités additionnelles d'utilisation et d'échange des données;
- la proposition de créer un système européen d'utilisation des données des passagers (PNR UE), qui obligera les compagnies aériennes à

communiquer aux autorités des États membres les données à caractère personnel de tous les passagers;

- deux décisions concernant l'échange entre les États membres des informations extraites des casiers judiciaires;
- la décision concernant l'accès des services répressifs au système d'information sur les visas;
- le cadre juridique relatif à SIS II.

Toutes ces initiatives législatives sont motivées par la nécessité, présumée inévitable, d'utiliser davantage d'informations. Depuis les attentats du 11 septembre 2001, la lutte contre le terrorisme est souvent à la base de ces mesures.

La focalisation de l'UE sur les informations et données à caractère personnel pourrait sembler logique dans la mesure où les institutions de l'UE n'ont pas la capacité d'assurer elles-mêmes directement la sécurité. Il n'y a pas de police européenne dotée de pouvoirs exécutifs. L'UE ne peut ordonner aux États membres de lutter contre des infractions spécifiques et les instances judiciaires européennes n'ont pas le pouvoir d'accorder une protection juridique directe aux personnes.

Par conséquent, l'UE continue de se focaliser sur les mesures censées permettre aux autorités compétentes des États membres de lutter contre la criminalité en utilisant une quantité accrue d'informations, dont des données à caractère personnel, ce qui est parfois hautement excessif.

Dans certaines circonstances, il est certes légitime et nécessaire, dans l'intérêt de la sécurité, de sacrifier jusqu'à un certain point le droit à la vie privée et d'autres droits fondamentaux. Notre société doit pouvoir se défendre au mieux contre certaines menaces.

Toutefois, il est indispensable que la charge de la preuve incombe toujours à ceux qui soutiennent que de tels sacrifices sont nécessaires et que toutes les mesures proposées constituent des instruments efficaces de protection de la société.

Les droits fondamentaux ne doivent pas être bradés uniquement pour créer uniquement l'illusion d'une sécurité accrue ou la mise en place de mesures exclusivement utiles à titre de précaution. Nous courons le risque de glisser imperceptiblement vers une société de la surveillance, petit à petit et sans percevoir toutes les conséquences d'une surveillance ancrée dans notre société, où les libertés et les droits fondamentaux seront, dans la pratique, fortement et définitivement réduits.

### *Les possibilités croissantes d'utilisation des informations*

Ceci m'amène aux possibilités croissantes d'utilisation des informations.

Les évolutions récentes dans le domaine des technologies de l'information et de la communication sont parfois considérées comme un motif autonome justifiant d'augmenter l'accès à et l'échange d'informations en vue de préserver la sécurité. Les TIC offrent aux organes répressifs de nouvelles et importantes possibilités d'accroître leur efficacité et d'utiliser de nouvelles stratégies proactives sur la base des informations disponibles et de la combinaison de ces informations.

Ces organes doivent indubitablement bénéficier des nouvelles technologies. Toutefois, tout instrument législatif, judiciaire ou administratif autorisant l'utilisation massive ou intelligente d'informations par les autorités répressives doit être fondé sur un choix spécifique, délibéré et transparent du législateur et, dans les cas sensibles, avoir fait l'objet d'un débat public.

Dans ce contexte, l'interopérabilité est une notion importante. La Commission semble aujourd'hui soutenir qu'il s'agit d'un concept plus technique que juridique ou politique. Cette explication est discutable. Elle repose sur l'hypothèse que le choix d'une technologie est un choix neutre et qu'il appartient aux utilisateurs de la technologie de fixer les conditions dans lesquelles son utilisation est permise.

Cependant, cette hypothèse ne tient pas compte du fait qu'une information a tendance à être utilisée si elle existe. Nous avons pu le constater avec la décision concernant l'accès des services répressifs au système d'information sur les visas, une base de données dont l'objectif n'a rien à voir avec le contrôle de l'application des législations. La Commission s'est également attelée à l'élaboration d'une proposition concernant l'accès à Eurodac, le système européen de comparaison des empreintes digitales des demandeurs d'asile.

### *Exemples de technologies de surveillance*

À ce stade, il me paraît utile d'entrer un peu plus dans les détails et de donner quelques exemples de technologies susceptibles d'affecter les personnes et leurs droits fondamentaux.

La technologie moderne de la vidéosurveillance en est un.

Les systèmes de vidéosurveillance sont de plus en plus sophistiqués et puissants.

De toute évidence, on observe une utilisation extensive de la surveillance par caméras de télévision en circuit fermé (CCTV) dans les espaces privés et semi-publics, en particulier dans les secteurs du transport et du commerce de détail.

De nouvelles initiatives sont en place, suivant l'exemple britannique de déploiement de CCTV dans la rue aux fins de prévention de la criminalité.

On peut argumenter que les CCTV ne sont que des caméras reliées par un câble à un écran d'affichage, qui facilite seulement l'observation humaine de la vie quotidienne, mais des décisions intéressantes émanant de la commission de Venise soulignent leur valeur ajoutée et démontrent qu'il est nécessaire de comprendre leur impact sur nos sociétés.

Les techniques de vidéosurveillance ont été initialement axées (notamment à partir des années 1970) sur la surveillance du trafic routier ou la prévention des vols simples ou qualifiés dans les banques et les magasins d'articles de luxe.

Dans les années qui ont suivi, les techniques de surveillance ont été spécialement perfectionnées en relation avec le lieu de travail, dans le secteur des transports — notamment dans les métros et les endroits situés à proximité — ainsi que dans certains bâtiments publics (pour empêcher le vandalisme) et espaces de loisirs.

Les techniques de surveillance ont ensuite connu un développement ininterrompu et ont trouvé des applications dans les secteurs les plus divers.

Dans le secteur des transports, le nombre de routes — routes nationales et autoroutes — contrôlées n'a cessé d'augmenter dans le but de surveiller le trafic, les délits (même au moyen de dispositifs infrarouges) et, plus récemment, l'accès aux centres-villes de toutes dimensions.

Des dispositifs de vidéosurveillance ont été largement installés dans les institutions bancaires, les stades et centres sportifs, les stations-service, les stations de taxis, les établissements de soins de santé, les musées et les cathédrales, les unités et quartiers résidentiels, ainsi que dans les lieux publics conçus pour promouvoir les activités touristiques.

Dans de nombreuses cités urbaines, il est difficile de trouver un endroit qui ne soit pas fortement surveillé.

Les systèmes modernes capturent et enregistrent des images numériques aisément copiables et diffusables. Les images peuvent être instantanément transmises à une multitude de destinataires ou publiées sur l'internet au moyen des puissants réseaux de communication numériques actuels et futurs.

Grâce à cela, des systèmes intelligents et interconnectés peuvent mieux comparer des images avec celles contenues dans une base de données ou suivre des cibles mobiles (objets ou personnes) dans de grands espaces. Leur capacité à identifier automatiquement un comportement «suspect» prédéfini est également meilleure.

De nouveaux outils d'intégration offrent la possibilité de combiner avec précision un nombre croissant d'informations collectées par une diversité plus grande de technologies de surveillance. Par exemple, il est possible de combiner l'interception de communications et la localisation de téléphones mobiles, des caméras de télévision en circuit fermé et des systèmes de reconnaissance de plaques d'immatriculation, des tickets de stationnement et des fichiers journaux accessibles en ligne. Il en résulte une analyse d'un torrent d'informations produites par des technologies de surveillance omniprésentes, avec un risque de divergences croissantes entre les scénarios suggérés et la réalité des faits.

### *Le besoin de protection*

L'utilisation croissante de données à caractère personnel entraîne — en tout cas dans un État de droit — un besoin croissant de protection. Un équilibre est nécessaire.

Dans une société de la surveillance, la protection est une grave préoccupation. Revenons à l'exemple des CCTV.

L'utilisation croissante de techniques de surveillance par un nombre toujours plus grand de magasins très fréquentés pourrait conduire à un

«détournement d'usage», facilitant l'utilisation d'images à des fins non prévues et non spécifiées initialement telles que l'analyse des habitudes du consommateur et de son comportement face à la disposition des produits en vente. Dans ce secteur spécifique, les systèmes de surveillance (et spécialement les systèmes de vidéosurveillance) sont devenus un instrument commercial précieux alors qu'ils avaient été initialement (ou apparemment) déployés dans le but de prévenir les vols simples ou qualifiés. L'utilisation de ces systèmes a ensuite permis de rationaliser les ressources, dans un point de vente déterminé (par exemple, en déterminant le nombre de caisses à ouvrir selon le moment de la journée et le nombre d'entrées) et dans une optique plus générale (par exemple, en élaborant des «circuits d'achat» susceptibles d'être jugés plus stimulants par les consommateurs).

Le fait d'être observé modifie notre comportement. En effet, se sachant observées, de nombreuses personnes peuvent avoir tendance à «censurer» leur langage et leur comportement, a fortiori dans le cas d'une surveillance largement répandue ou continue. Savoir qu'une caméra suit tous nos faits et gestes peut avoir un impact psychologique et modifier les comportements. Il y a là interférence avec notre vie privée.

La liberté d'expression pourrait s'en trouver menacée: un système de CCTV peut par exemple décourager des comportements légitimes tels que des protestations politiques contre des mesures impopulaires. Traditionnellement, toute personne a le droit de participer anonymement à un rassemblement pacifique, sans risque d'identification et de conséquences. Cette situation subit des changements fondamentaux.

Le fait « d'être vu sans voir » peut influencer la conduite et l'activité d'une personne. D'une part, les dispositifs cachés de capture d'images et/ou de contrôle ne favorisent pas la franchise de la part des citoyens. D'autre part,

le fait d'avoir connaissance de l'installation de caméras et autres dispositifs sur un site peut entraîner un comportement «docile» de la part des citoyens.

Voyons maintenant l'impact sur la liberté de circulation: les systèmes modernes de CCTV équipés de systèmes de reconnaissance faciale et/ou les logiciels de surveillance préventive dynamique intégrés dans de gros systèmes interconnectés peuvent suivre les mouvements des personnes dans de vastes espaces. Il faut en réalité insister sur le fait que la liberté de circulation signifie la liberté de se déplacer physiquement mais aussi, dans un sens plus fondamental, la liberté de se déplacer sans devoir inévitablement laisser des traces continues et/ou fréquentes utilisables par des «informateurs optiques» permanents.

Passons à l'impact sur le droit à la non-discrimination: les opérateurs de CCTV pourraient être tentés de concentrer la surveillance sur les minorités ethniques, les adolescents, les sans-abri et tous les groupes de personnes non conformistes perçus comme «à risque».

Les occasions de violations de la sécurité et d'abus se multiplient: les enregistrements peuvent tomber dans de mauvaises mains ou être utilisés à des fins illicites par les destinataires légitimes.

Le développement technique de ces systèmes a progressivement permis la transmission d'images à des «centres de contrôle», l'association d'images et de sons et l'introduction de «systèmes intelligents» d'analyse et d'intervention.

Les systèmes de surveillance peuvent être équipés de ou associés à des logiciels de recherche automatisée d'images, permettant l'identification par des techniques conçues pour le ciblage d'auteurs présumés d'infractions — par exemple, les techniques de reconnaissance faciale automatique (applications logicielles de texturage facial).

Il devient de plus en plus aisé de lancer divers types d'alerte (y compris le signalement aux gardiens) concernant des personnes suspectes sur la base de descriptions spécifiques ou de traits de comportement automatiquement classés comme «anormaux» par le logiciel (par exemple, dans une aire de stationnement ou à l'entrée d'un stade).

Cela suggère l'identification possible de cas d'inconduite présumés sur la base de l'apparence physique (caractéristiques physiques, habillement, couleur de peau) ou d'actions et événements considérés comme particulièrement intéressants (mouvements brusques, fumée, ouverture de portes).

Peut-on affirmer qu'il s'agit dans tous les cas de solutions proportionnées à nos problèmes contemporains et que tout cela est nécessaire et approprié?

Certes, les systèmes de surveillance peuvent avoir des effets positifs en termes de sécurité; cependant, la mesure dans laquelle cet effet peut être jugé positif n'est pas uniforme. Dans quelques cas, il y a indubitablement eu une diminution du nombre de délits dans les lieux publics; dans d'autres, cette surveillance s'est avérée inefficace ou a conduit les criminels à se déplacer vers d'autres zones proches; dans d'autres cas encore, la surveillance a simplement permis d'obtenir des preuves contre les personnes filmées. Enfin, il y a le risque qu'une surveillance soit mise en place dans une mesure excessive comme moyen pratique de contrer des failles d'organisation ou de répression et non pour répondre à des exigences réelles.

Si le respect du principe de proportionnalité n'est pas garanti, le nombre de lieux publics et privés sous surveillance pourrait augmenter de manière exponentielle dans les prochaines années: le résultat final serait une société imposant des restrictions excessives à la liberté individuelle. En d'autres termes, la surveillance devrait être limitée aux lieux réellement à risques.

La nécessité absolue d'adopter pour l'avenir une approche plus sélective en ce qui concerne l'utilisation de systèmes de surveillance ne peut faire aucun doute: il est inconcevable que toute une population subisse des limitations excessives de ses droits en raison du besoin d'empêcher l'inconduite d'une minorité de cette population.

Il faut dès lors élargir le débat au-delà de la question des effets bénéfiques pour la sécurité des personnes et des biens: il serait plus approprié d'évaluer aussi les effets de la surveillance sur la liberté et la conduite des citoyens.

En d'autres termes, outre l'examen de la mesure dans laquelle la surveillance engendre une violation de la vie privée, l'évaluation des effets d'une large utilisation de la surveillance sur la libre circulation et le comportement des citoyens est également requise.

Les citoyens peuvent donc être transformés en «sujets» d'information, sans respect du droit à l'autodétermination informationnelle.

### *La notion plus générale de surveillance*

Ces arguments sont également pertinents en relation avec la notion plus générale de surveillance, qui est très vaste par nature et va bien au-delà du contrôle au moyen d'équipements vidéo. Cette notion englobe le contrôle des communications téléphoniques et informatiques ainsi que le contrôle de la circulation de contenus. Elle peut même s'appliquer au contrôle à distance d'utilisateurs spécifiques d'un service (par exemple, la localisation de téléphones mobiles) ou de personnes concernées par une action judiciaire (c'est le cas avec l'utilisation de bracelets électroniques).

La notion de surveillance pourrait en effet désigner *«toute activité opérée par des moyens techniques, consistant à surveiller, collecter et/ou enregistrer, de*

*façon non occasionnelle, des données à caractère personnel concernant un ou plusieurs individus et relatives à leurs comportements, mouvements, communications et utilisation de dispositifs informatiques et/ou électroniques».*

L'émergence de «l'informatique en nuage» et de ses services à distance connexes en est un exemple clair. Si un mandat judiciaire est éventuellement nécessaire pour accéder à l'ordinateur familial au domicile privé, dans certains pays, ce n'est parfois pas le cas lorsque certains logiciels sont installés dans un PC ou lorsque des informations auparavant stockées «chez soi» sont désormais détenues ou traitées à l'extérieur par un serveur central. La technologie va offrir énormément de possibilités en termes de surveillance, étant donné que la plupart de nos activités seront visibles « de l'extérieur » ou « en ligne ».

Il serait utile de se demander si une lutte efficace contre la criminalité nécessite de réduire les droits et libertés fondamentales des citoyens qui ne sont pas concernés par les enquêtes effectuées par des organes publics.

Nous devons évaluer le besoin spécifique d'appliquer des techniques d'enquête qui affectent non seulement la vie privée de terroristes, mais aussi celle de millions d'autres personnes qui ne sont aucunement impliquées dans des activités criminelles.

Il est possible de tenir un raisonnement plus équilibré. Il convient de réfuter l'équation «plus de sécurité = moins de vie privée» et de partir du principe que la vie privée n'est pas un obstacle à la sécurité.

En effet, l'urgence liée à de véritables activités terroristes à un moment donné de l'histoire — en particulier s'il s'agit d'activités de grande envergure comme celles qui ont eu lieu à New York, Washington, Londres et Madrid — est une chose, tandis que les exigences typiques de tout service répressif poursuivant — dans des circonstances ordinaires, c'est-à-dire dans le cadre de

ses enquêtes normales — des délits tels que la pornographie infantile, la cybercriminalité, les comportements xénophobes, le blanchiment d'argent, parfois en collectant une masse de données en lignes, sont totalement différentes.

Il y a également un risque de voir réapparaître dans certains pays la méthode «Rasterfahndung», c'est-à-dire l'analyse systématique de données, appliquée dans les années 1970 contre la RAF. Cette approche repose sur le recoupement de données sur la base d'une série de critères permettant de définir des profils de criminels potentiels — par exemple, le règlement des factures d'eau et d'électricité en liquide et non par virement bancaire, les retards de paiements ou la perte d'un passeport — et d'examiner des circonstances «anormales» considérées comme nécessitant une analyse plus approfondie. La vie de personnes non suspectées est ainsi progressivement passée au crible.

Les étrangers musulmans font aujourd'hui l'objet d'une analyse généralisée sur la base d'informations telles que les données administratives d'abonnements, les consommations d'électricité/d'eau/de gaz/de téléphone — normales et atypiques — les modes de paiement (virements bancaires, paiement en liquide, etc.). D'énormes quantités de données sont analysées, puis stockées, au sujet de personnes qui, bien qu'il ne soit pas toujours certain qu'elles doivent être identifiées — seront certainement identifiables à l'issue de cette analyse.

En décembre dernier, lors d'une session au Parlement européen, Jacques Barrot, vice-président de la Commission, a mentionné le projet de prise d'empreintes digitales dans les camps nomades en Italie afin de souligner les récentes initiatives européennes et nationales visant à rétablir le plein respect du droit communautaire et des droits fondamentaux.

D'autres exemples peuvent être cités (hormis le dossier PNR), comme l'établissement de «no-fly lists» — c'est-à-dire de listes de personnes interdites de vol commercial à destination de ou au départ d'un pays —, ou encore la collecte illégale, masquée et massive, d'adresses de sites internet par certains fournisseurs d'accès à l'internet et la nouvelle législation imposant de fournir aux utilisateurs internet des adresses IP non équivoques.

Les sociétés véritablement démocratiques doivent s'engager dans cette lutte, mais il y a des conditions à respecter.

Des critères de proportionnalité doivent être respectés.

Nous devons agir avec sagesse: si les mesures envisagées peuvent avoir des répercussions négatives sur les droits fondamentaux, il importe de se limiter aux mesures qui ne sont pas simplement utiles ou désirables, mais qui respectent réellement les exigences sociales impératives - comme l'a également arrêté la Cour européenne des droits de l'homme.

Il convient que nous examinions l'impact à long terme des mesures et initiatives que nous prenons.

Il convient que nous engagions dans nos sociétés un débat ouvert et le plus large possible sur les initiatives en matière de lutte contre la criminalité afin d'évaluer toutes leurs conséquences concrètes sur les libertés et les droits fondamentaux.

Nous devons nous abstenir d'adopter des dispositions obscures et incomplètes et accorder la priorité aux mesures aisément accessibles et prévisibles en termes de portée et de modalités d'application.

Nous devons réussir, je le répète, à établir une distinction entre les mesures antiterroristes et celles dont le champ d'application est beaucoup plus large — par exemple, les cartes d'identité, l'utilisation à grande échelle des identifiants biométriques ou la définition générique de la «criminalité

informatique», qui autorise des interprétations dérogeant aux principes de l'État de droit (voir la récente convention du Conseil de l'Europe relative à la cybercriminalité).

Est-il bien opportun d'exiger des dispositifs de sécurité biométriques pour identifier les personnes voyageant fréquemment par avion alors qu'un seul coup d'œil nous suffit à nous, pigeons voyageurs — ou, si vous préférez, victimes de voyages fréquents —, pour nous reconnaître les uns les autres dans les halls et les salles d'attente des aéroports?

Si des données biométriques sont requises aux fins d'identification, pouvons-nous être certains à 100 pour cent qu'aucune autre technique n'est disponible pour procéder à une identification sans risque?

Avant d'instaurer de nouvelles mesures de lutte contre le terrorisme, nous devrions plutôt nous efforcer de déterminer avec soin s'il n'existe pas des approches moins intrusives pour la vie privée pour établir des faits et des responsabilités.

Nous devrions demander aux autorités compétentes et aux entités privées concernées par ces mesures — plus particulièrement dans le secteur des télécommunications — d'évaluer leur proportionnalité par rapport à la nature et à la gravité des infractions pénales, de manière à éviter les bases de données faisant double emploi.

S'il apparaît qu'il est suffisant que certaines données soient accessibles en ligne, il est inutile d'autoriser d'autres entités à créer des banques de données distinctes.

L'excès de points d'accès en ligne réduit la sécurité des systèmes d'information.

Il convient également de réfléchir au fait que les bases de données regorgeant d'informations collectées à titre de précaution sont loin d'être efficaces parce que saturées d'informations «parasites».

Nous devons renoncer à tout type de surveillance généralisée et établir des protections contre d'éventuelles initiatives arbitraires de la part des autorités publiques.

### *Activités d'enquêtes: preuves et médias électroniques*

Dans cette perspective, la mise en œuvre de la convention de Budapest sur la cybercriminalité constitue un autre exemple important.

Cette convention ne s'applique pas seulement à la cybercriminalité, étant donné qu'elle aborde également les procédures et mécanismes concernant diverses activités d'enquête pénale (inspections, fouilles, saisie de courriers et autres objets, garde à vue, enquêtes urgentes, etc.) liées à d'autres types d'infractions — c'est-à-dire des infractions «traditionnelles» — chaque fois que les preuves nécessaires figurent sur des médias électroniques ou doivent être recueillies à l'aide de médias électroniques.

La convention de Budapest envisage divers mécanismes de coopération et d'assistance mutuelle, y compris à des fins d'extradition. Ces mécanismes s'appliquent non seulement aux infractions pénales «*en relation avec des systèmes et des données informatiques*», mais aussi à la «*collecte des preuves électroniques*» d'une infraction pénale. Ceci peut concerner un nombre considérable de cas, étant donné que les infractions en question sont passibles d'une peine privative de liberté pour une période maximale d'au moins un an.

Avec un tel cadre, les enquêtes pénales menées dans les différents pays — y compris les enquêtes résultant de demandes de coopération internationale en vertu de la Convention — pourraient aboutir à la collecte et

à l'échange d'une quantité considérable de données à caractère personnel (y compris les données relatives aux communications internet et téléphoniques) qui ne sont pas nécessairement associées directement à la cybercriminalité ou qui pourraient concerner des activités totalement licites.

La Convention ne tient compte que partiellement des objections et suggestions formulées par les autorités de l'Union européenne chargées de la protection des données en termes de nécessité, d'adéquation et de proportionnalité.

Les mesures d'assistance doivent prévoir la protection adéquate des droits de l'homme fondamentaux — en particulier ceux établis par la Convention européenne des droits de l'homme, dont l'article 8 fait référence au droit au respect de la vie privée. Ces mesures doivent en outre respecter «le principe de proportionnalité».

L'application du principe de proportionnalité est présentée par la Convention comme une nécessité impérative en vue d'une application appropriée de la Convention proprement dite.

Par conséquent, il importe d'inclure ce principe (si ce n'est pas encore le cas) ou de le développer de manière appropriée dans la législation nationale. À cette fin, chaque texte législatif réglementant les enquêtes et le travail préparatoire en relation avec des procédures pénales devrait contenir une disposition ad hoc prévoyant que les activités d'enquête et de procédure devront être effectuées par les autorités judiciaires et/ou policières selon une approche proportionnelle et sélective — c'est-à-dire, en vérifiant que les données et informations sont pertinentes et non excessives au regard des enquêtes en cours et en appliquant des mécanismes tout aussi proportionnés. Une autre solution consisterait à envisager une règle générale unique qui figurerait dans l'acte de ratification de la Convention et serait ultérieurement intégrée dans la législation relative à la procédure pénale.

Les clauses de «proportionnalité» en question doivent également s'appliquer aux autres activités d'enquête mentionnées dans la Convention, qu'elles soient ou non déjà réglementées par le droit national — par exemple, en ce qui concerne l'Italie, à l'interception des communications et conversations, en particulier aux techniques d'écoute téléphonique de «nouvelle génération» telles que celle appliquées à la téléphonie par internet.

S'il s'avérait impossible de garantir la mention explicite du principe de proportionnalité dans les actes juridiques réglementant les enquêtes, il serait sans aucun doute approprié de sensibiliser les autorités compétentes chargées des enquêtes afin de garantir le respect constant du principe de proportionnalité mentionné dans la Convention durant les enquêtes, y compris par rapport aux sites internet, blogs, réseaux sociaux, espaces et forums de discussion.

En ce qui concerne l'impact des activités d'enquête sur les droits des tiers, je pense que dans chaque pays, la législation devrait aussi comporter une disposition prévoyant un principe similaire à celui établi par l'article 15 de la Convention, qui impose d'examiner l'effet des procédures d'enquête sur les droits et intérêts légitimes des tiers. Il est pratiquement hors de doute que l'utilisation de moyens informatiques — susceptibles de faire l'objet d'une saisie — facilite le traitement d'une énorme quantité de données à caractère personnel concernant également d'autres personnes. Ceci entraîne la nécessité d'une approche particulièrement sélective dans le cadre de la réalisation de l'enquête pour éviter également d'affecter les droits et intérêts particuliers d'individus n'ayant rien à voir avec les faits sur lesquels porte l'enquête.

Enfin, en ce qui concerne le gel des données relatives aux communications, la Convention de 2001 ne contient pas de dispositions imposant aux fournisseurs de services de communications électroniques de conserver systématiquement ces données.

La Convention n'autorise en effet que la conservation temporaire de données informatiques spécifiques — dont les données relatives aux communications — déjà en possession de ou sous le contrôle des fournisseurs de services (ce qu'on appelle le «gel» des données), y compris aux fins d'une coopération internationale. Cette mesure est applicable s'il s'avère nécessaire que les autorités compétentes disposent de ces données et qu'il existe des motifs de penser que les données informatiques sont particulièrement susceptibles de perte ou de modification.

Le «gel» des données est particulièrement approprié dans les systèmes juridiques qui n'autorisent pas une conservation à grande échelle des données relatives aux communications (par exemple, ceux qui appliquent la directive 2006/24/CE) ou qui n'autorisent une telle conservation que pour une durée très limitée.

Toute mesure relative à cet aspect doit être soigneusement évaluée à la lumière des principes de limitation de la finalité et de proportionnalité —étant donné que la législation en question s'appliquerait également aux données autres que les données de facturation — et conformément à une approche sélective. Il convient en outre de tenir compte des dispositions de la Convention (article 15, paragraphe 2, article 16, paragraphe 1, et article 29) relatives aux conditions et durées de conservation des données. Les Etats membres de l'UE devraient également faire référence aux garanties prévues dans la directive européenne sur la conservation des données relatives aux communications.

### *La reconnaissance juridique de la protection*

Nos traditions juridiques confèrent à la protection des données et au droit à la vie privée le caractère de droits fondamentaux. Citons à cet égard la Convention européenne des droits de l'homme, la Charte des droits fondamentaux de l'Union européenne, le traité CE et les constitutions d'un

certain nombre d'États membres. L'instrument législatif le plus connu en matière de protection des données est, évidemment, la directive 95/46.

Tous les nouveaux actes juridiques de l'UE relatifs à l'utilisation de l'information — je les ai mentionnés tout à l'heure — doivent respecter les principes de la protection des données pour satisfaire aux conditions énoncées à l'article 6, paragraphe 1, du traité sur l'Union européenne.

De plus, dans le troisième pilier, l'article 30, paragraphe 1, point b), du TUE, dispose que l'action en commun dans le domaine de la coopération policière relative à la collecte (etc.) d'informations est autorisée «sous réserve des dispositions appropriées relatives à la protection des données à caractère personnel».

Le troisième considérant de la nouvelle décision-cadre du Conseil relative à la protection des données (2008/977/JAI) annonce des normes communes contribuant à l'efficacité de la coopération policière et judiciaire, à sa légitimité et au respect des droits fondamentaux.

Ce ne sont là que quelques exemples d'un cadre perfectionné.

L'important arrêt récent dans l'affaire *S. et Marper contre Royaume-Uni* illustre sans doute le mieux l'équilibre nécessaire entre l'utilisation d'informations et la protection des données.

Dans cette affaire, la Cour européenne des droits de l'homme a considéré que le stockage d'empreintes digitales et de profils ADN par les autorités du Royaume-Uni constitue une violation de l'article 8 de la Convention européenne des droits de l'homme. Le système autorisait la conservation illimitée des empreintes digitales et du matériel ADN de toute personne, de n'importe quel âge, soupçonnée d'avoir commis une infraction — même mineure — emportant inscription dans les fichiers de la police.

La Cour a également mentionné le risque de stigmatisation, qui découle du fait que certaines personnes qui n'ont été reconnues coupables d'aucune infraction sont traitées de la même manière que des condamnés.

### *La technologie et la communication de la Commission du 10 juin 2009*

J'ai commencé par un regard sur la communication de Stockholm de la Commission et je reviens sur cet aspect pour conclure ma présentation. Je ne vais pas analyser ici la communication — elle est toute récente et le CEPD rendra un avis dans les prochaines semaines. Toutefois, il est judicieux de souligner les orientations envisagées actuellement par la Commission.

Selon moi, cette communication témoigne d'une grande ambition en ce qui concerne la question de l'équilibre entre surveillance et protection. Elle aborde les technologies sous plusieurs angles, à savoir:

1. Les développements technologiques et l'amélioration de l'utilisation de moyens technologiques permettant la surveillance des citoyens.
2. Les développements technologiques en relation avec les droits fondamentaux — en particulier la protection des données — en tant que condition nécessaire dans l'espace de justice, de liberté et de sécurité.
3. La technologie en tant qu'outil permettant une meilleure coopération judiciaire.

#### L'utilisation des moyens technologiques:

- Un des objectifs mentionnés est de mobiliser les outils technologiques nécessaires, par exemple par la sécurité de l'information, l'interopérabilité avec les systèmes européens existants et

- La communication vise à étoffer le système européen d'information sur les casiers judiciaires (ECRIS) au moyen d'un registre de données concernant les ressortissants de pays tiers (4.2.2).

- Le développement du système d'information de Schengen de deuxième génération (SIS II) et du système d'information sur les visas (VIS) sera finalisé et un système d'enregistrement électronique des entrées dans les États membres et des sorties sera établi et couplé à un programme d'enregistrement des voyageurs (4.2.3.2).

- Une meilleure approche à l'égard de la cybercriminalité et des attaques informatiques est annoncée.

- L'utilisation de l'internet à des fins de terrorisme doit faire l'objet d'une surveillance accrue (4.3.2).

La protection des données, en tant que condition nécessaire:

- Des nouvelles technologies appropriées peuvent garantir le respect de la protection des données (point 2.3 de la communication).

- L'Union doit établir un régime complet de protection des données à caractère personnel couvrant tous les domaines de compétence de l'UE.

- La mise en place d'un système de certification européenne pour les technologies, les produits et les services «respectueux de la vie privée» doit être examinée. Les technologies «respectueuses de la vie privée» sont généralement celles qui prennent en compte la vie privée dès la conception (principe de «privacy by design»).

- La protection des données exige une coopération internationale solide. L'Union doit contribuer au développement et à la promotion de normes internationales dans ce domaine.

La technologie sera également utilisée en tant qu'outil permettant une meilleure coopération judiciaire: le projet «Justice en ligne» (e-Justice) est présenté comme un moyen de donner aux citoyens un accès à la justice. Il offrira un portail d'information, le recours à la vidéoconférence en tant qu'élément de la procédure judiciaire, la possibilité de procédures en ligne et l'interconnexion de registres (3.4.1). Les échanges entre professionnels auront lieu à travers le Forum européen pour la justice.

Je vous remercie de votre attention et vous prie de m'excuser d'avoir omis d'aborder ici le développement juridique le plus passionnant pour la protection des données dans l'UE: nous pourrons en effet bientôt travailler, espérons-le, sur la base du traité de Lisbonne. Ce traité nous offrira un meilleur cadre pour concilier liberté, sécurité et justice, c'est-à-dire les valeurs essentielles faisant partie intégrante du modèle de société européen.

Considérer le droit à la vie privée comme un obstacle à la lutte efficace contre le terrorisme ou même comme l'agneau à sacrifier est une erreur.

Comme le prône le rapport publié le 3 juin dernier par la commission des lois du Sénat français, il est nécessaire de développer des solutions modernes, adéquates et durables pour répondre aux défis spécifiques de notre ère numérique.