COMMISSAIRE AUX DROITS DE L'HOMME

CONSEIL DE L'EUROPE

Strasbourg, 10 décembre 2008

CommDH/IssuePaper(2008)3
Or.anglais

LUTTE CONTRE LE TERRORISME ET PROTECTION DU DROIT AU RESPECT DE LA VIE PRIVEE

TABLE DES MATIERES

Les *documents thématiques* publiés par le Commissaire aux droits de l'homme ont pour objet de donner un coup de projecteur sur certain sujets d'actualité sous l'angle des droits de l'homme. Ils en présentent les principales données de fait et de droit. Le cas échéant, ils soulèvent des questions, proposent des pistes de travail et formulent des suggestions ou des mises en garde. Ces documents ont essentiellement vocation à informer – les citoyens, les pouvoirs publics et les membres d'organisations non gouvernementales œuvrant dans le domaine de la protection des droits de l'homme – et à stimuler le débat. Ils n'ont pas la valeur d'une recommandation ou d'un avis tels que prévus par le mandat du Commissaire. Tous les documents thématiques sont disponibles sur le site web du Commissaire.

Remerciements

Le Commissaire aux droits de l'homme tient à remercier le professeur Douwe Korff, de la Metropolitan University de Londres, pour sa contribution à l'élaboration de ce document en tant que consultant externe de son bureau.

1. Introduction

Garanti par l'article 8 de la Convention européenne des droits de l'homme, le droit au respect de la vie privée englobe un droit plus spécifique généralement désigné par l'expression « protection des données », qui ne se limite pas à la protection des individus contre les intrusions dans leur vie privée. Plus généralement, ce droit vise à les protéger contre la collecte, le stockage, l'échange et l'utilisation impropres de données les concernant. Il porte sur la question – centrale dans la société de l'information – de l'étendue du pouvoir que peuvent exercer les responsables du traitement des données sur les personnes concernées par un traitement de données du fait qu'ils possèdent des données à caractère personnel sur elles. L'affirmation de ce droit ne cesse de se confirmer, notamment dans la jurisprudence de la Cour européenne des droits de l'homme et de la Cour européenne de justice.

Bien que le terrorisme ait été au centre des préoccupations, notamment depuis le 11-Septembre, il n'en existe toujours pas de définition universelle précise. Peut-être parce qu'il n'y a pas de consensus possible au niveau mondial sur ce qui distingue un terroriste d'un combattant de la liberté. Pour l'Union européenne, doivent être considérés comme infractions terroristes les actes ou les menaces visant à

> […] gravement intimider une population ou contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque ou gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou une organisation internationale. (Décision-cadre 2002/475/JAI, article 1)

Cela étant, ni la Convention européenne pour la répression du terrorisme (Conseil de l'Europe, 1977), ni la Convention internationale pour la répression des attentats terroristes à l'explosif (ONU, 1997) ne définissent le terme « terrorisme ». Le Conseil de sécurité de l'ONU n'a pas non plus adopté de définition alors même qu'il prescrit des sanctions contre des « terroristes » (présumés).

Les problèmes évoqués dans le présent document s'inscrivent donc dans un contexte qui présente la double particularité d'être extrêmement sensible et mal défini. D'une part, ils touchent aux valeurs fondamentales de toute société démocratique et posent des questions constitutionnelles cruciales dans de nombreux Etats. D'autre part, ils ont trait à un phénomène, le terrorisme, face auquel les Etats se sentent en droit, et même obligés, de prendre les mesures les plus drastiques.

Quelle que soit la définition retenue, le terrorisme est un phénomène qui résiste au temps. Alors que les guerres et autres situations de crise connaissent généralement une fin plus ou moins claire (même si elle tarde parfois beaucoup à venir), rien ne permet de prévoir la fin de la lutte contre le terrorisme à l'échelle mondiale. Même au niveau national, les législations antiterroristes ont tendance à se pérenniser.

Le terrorisme et les mesures antiterroristes constituent donc une menace persistante pour les valeurs fondamentales du Conseil de l'Europe et de ses Etats membres. Le risque porte en particulier sur la collecte, le stockage, l'analyse, l'échange et l'utilisation de données à caractère personnel. La protection des données est souvent perçue comme un obstacle à l'application concrète de mesures antiterroristes et c'est donc l'un des principaux domaines dans lesquels les engagements internationaux ne sont pas respectés. Or la protection des données est essentielle pour la défense des grandes valeurs démocratiques. La difficulté du problème tient aux contradictions fortes entre la volonté d'empêcher le terrorisme de frapper et la nécessité de protéger les droits de l'homme.

Un accord entre le Conseil de l'Europe et l'Union européenne est intervenu il y a peu en faveur de la coopération, « notamment dans la lutte contre le terrorisme, la criminalité organisée, la corruption, le blanchiment d'argent et d'autres défis modernes, y compris ceux résultant du développement de nouvelles technologies ».[1] Le Commissaire aux droits de l'homme fait partie des organes

[1] Mémorandum d'accord entre le Conseil de l'Europe et l'Union européenne, adopté à la 117e Session du Comité des Ministres (Strasbourg, 10-11 mai 2007), Document du Conseil de l'Europe CM(2007)74 du 10 mai 2007, par. 26 (dans la partie intitulée « Prééminence du droit, coopération juridique et réponse aux nouveaux défis »).

« particulièrement invités » à participer au renforcement de cette coopération.[2] Les problèmes de droits de l'homme posés par les mesures relatives à la vie privée et à la lutte contre le terrorisme et, plus généralement, par les technologies de l'information, sont donc du ressort du Commissaire.

2. Etat de l'art

Les réponses apportées au terrorisme dépendent fortement des progrès technologiques qui se présentent sous diverses formes de plus en plus imbriquées. Premièrement, de nouvelles technologies de surveillance directe se font jour : systèmes de vidéosurveillance wifi haut débit et haute définition, combinés à des logiciels de reconnaissance du visage (et de la démarche) ; des caméras de surveillance autoroutière capables de lire les plaques d'immatriculation et de suivre l'itinéraire de certains véhicules ; technologies de surveillance, de filtrage et d'analyse de milliards de communications téléphoniques et de courriers électroniques en temps réel ; technologies d'écoute et de pistage presque indétectables ; logiciel espion installé subrepticement sur l'ordinateur d'un suspect par les autorités qui peuvent alors surveiller à son insu et à distance toutes ses activités en ligne et sa messagerie électronique, se procurer ses mots de passe et même activer la caméra et le micro de l'ordinateur.

Le rôle de ces dispositifs ne se limite plus à la simple observation : des logiciels censés identifier les « comportements suspects », voire détecter « l'intention hostile » d'une personne, ont d'ores et déjà été mis au point par des Etats et des entreprises ou sont en cours de développement. Les ordinateurs de surveillance ne se contentent plus d'observer, ils attirent l'attention de la police et d'autres autorités sur des « cibles » particulières.

Deuxièmement, la surveillance des personnes par les données (on parle en anglais de *dataveillance*) est en plein essor : elle consiste à suivre les pistes laissées sous forme de données par les personnes lors de nombreuses transactions nécessitant un accès à des bases de données publiques ou privées. Ces dernières peuvent être des bases de données commerciales (fichiers clients de sociétés, données de communication, etc.) D'autres dépendent du secteur semi-public. Dans plusieurs pays, on a recours aux empreintes digitales (ou au contour de la main) pour contrôler l'accès aux bibliothèques et aux cantines scolaires. De plus, les Etats constituent eux-mêmes des bases de données nationales toujours plus volumineuses, dans lesquelles ils stockent des données biométriques (photographies faciales lisibles par ordinateur, empreintes digitales, profils d'ADN, etc.) Au Royaume-Uni, on prélève l'ADN de toute personne arrêtée et placée en détention, même si elle est innocentée. Dans de nombreux pays, il existe des bases de données nationales contenant des informations relatives à l'assurance maladie, aux retraites et aux prestations sociales. Ceux qui possèdent des bases de données centralisées contenant les dossiers médicaux d'importants groupes de population sont de plus en plus nombreux. D'autres bases contiennent toutes les informations de police concernant indifféremment suspects, victimes ou témoins. Le citoyen n'est pas libre de fournir ou non ces informations, et cette manière de forcer les choses ne cesse de gagner du terrain à l'échelle internationale. Ainsi, le Règlement (CE) n° 2252/2004 du Conseil prévoit la prise et la conservation des empreintes de tous les détenteurs de passeports de l'Union européenne – autrement dit, de centaines de millions de citoyens européens innocents. De la même manière, des données à caractère personnel sont soutirées d'office aux voyageurs qui prennent l'avion pour être analysées et traitées à des fins antiterroristes.

Combiner ces bases de données et les relier à d'autres (par exemple, à des bases sur le style de vie des consommateurs alimentées par des sociétés d'extraction de données, des sociétés de renseignement commercial ou des agences de voyages) permet de brosser un tableau d'une précision naguère inimaginable de nos vies, de nos centres d'intérêt, de nos attaches culturelles, de nos convictions politiques et religieuses, de notre situation financière et de notre santé. Les garanties offertes en matière de protection des données contre le transfert sont d'autant plus faibles que la législation antiterroriste contribue à les réduire. L'individu se trouve de plus en plus démuni face aux autorités nationales et internationales.

[2] *Idem*, par. 47 (dans la partie intitulée « Coopération inter-institutionnelle »).

Troisièmement, la police et les services secrets explorent les bases de données à la recherche d'individus correspondant à un profil prédéterminé (mais mis à jour dynamiquement). De plus en plus, ces recherches sont fondées sur le renseignement d'une part et menées dans le cadre de politiques européennes et non plus exclusivement nationales d'autre part.

Beaucoup de ces technologies sont manifestement porteuses de menaces pour notre vie privée et nos libertés en ce qu'elles permettent à l'Etat de surveiller étroitement nos vies. Cependant, elles sont loin d'être sans faille et ne sont pas exemptes de sérieuses limitations qui leur sont parfois même inhérentes. Toutes les personnes qui pourraient remettre en cause les dispositions existantes entre les autorités et l'industrie de pointe (membres de commissions parlementaires, de groupes de défense des droits civils, de l'opposition politique, etc.) ne sont souvent pas à même de le faire, faute d'une compréhension suffisante des détails techniques et des conséquences possibles (sans compter qu'on refuse souvent de leur communiquer les détails techniques « pour protéger le secret commercial »). Plus la technologie d'un produit est pointue, plus il est difficile d'évaluer ses caractéristiques revendiquées et ses faiblesses.

Les technologies sur lesquelles repose le profilage et l'extraction des données ne semblent bien fonctionner que jusqu'à un certain point mais vont inévitablement à l'encontre des intérêts d'une multitude d'innocents dans une mesure inacceptable dans une société démocratique et dans des proportions qui rendent la « pêche » inefficace. Il importe de souligner la nature inéluctable de ce phénomène auquel les améliorations apportées à la conception des produits ne sauraient mettre fin. D'un point de vue statistique, il est certain que les tentatives d'identification d'incidents ou de cibles très rares dans un énorme volume de données ne peuvent déboucher que sur un taux inacceptable de faux positifs (désignant des innocents comme suspects) ou de faux négatifs (échec de l'identification des véritables criminels ou terroristes). Aux Etats-Unis, le *National Research Council* a publié très récemment un rapport de référence qui conclut que l'identification automatisée des terroristes par extraction de données (ou toute autre méthode connue) n'est ni un objectif réalisable, ni une perspective souhaitable pour la recherche technologique.[3]

3. Intensification de la coopération policière

En Europe, la police est de plus en plus considérée comme l'un des éléments d'un pacte social élargi dans le cadre duquel les politiques publiques sont mises en œuvre globalement. On tend en effet à mettre l'accent sur la prévention et à combiner l'action de la police et de la justice avec des approches sociales plus larges.

Cette conception reposant sur un pacte sociétal suppose une multiplication considérable des échanges de données entre la police et les autres administrations comme les services sociaux ou d'éducation. Il ne fait pas de doute que les politiques « communes » et la coordination des travaux des différents services présentent des avantages mais ces dispositifs de collecte et d'échange de données risquent d'aboutir à une culture de la surveillance quasi généralisée.

Autre changement de grande ampleur dans le monde policier, l'évolution des relations entre la police et les services secrets dans plusieurs pays. Outre les informations obtenues grâce aux technologies avancées de surveillance des personnes et des données les concernant (voir ci-dessus), ou auprès des services secrets, des renseignements proviennent également d'agents secrets et d'informateurs. Par conséquent, on connaît de moins en moins les raisons pour lesquelles la police (et d'autres services) s'intéressent à une personne et la nature des éléments de preuve réunis contre cette

[3] *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, rapport du National Research Council (institut national de recherche américain), 2008, résumé, pages 3-4. Cette idée est expliquée de manière plus détaillée dans le corps du rapport, selon lequel l'identification automatisée de terroristes n'est pas techniquement réalisable car la notion d'élément anormal - en l'absence d'idée précise de ce qu'est un élément de menace - risque d'être associée à de nombreuses activités moins graves que le terrorisme. Le nombre de fausses pistes pourrait alors épuiser toutes les ressources d'investigation ou d'analyse. C'est pourquoi l'intérêt d'orienter l'évolution technologique vers l'identification automatisée des terroristes est extrêmement discutable. (pages 78-79). Pour consulter l'évaluation in extenso, voir l'annexe H du rapport, intitulée *Data Mining and Information Fusion*. Le rapport est disponible à l'adresse suivante : http://www.nap.edu/catalog.php?record_id=12452 (en anglais).

personne. Cette situation a des répercussions directes sur la manière dont peut être traitée n'importe quelle personne, qui risque d'être espionnée, harcelée ou arrêtée, à qui l'on peut refuser un emploi ou un poste de chercheur[4] - sans qu'elle en connaisse les raisons ou qu'elle puisse mettre en cause ces mesures (et parfois même à son insu). Le rapprochement entre la police et les services secrets risque aussi de nuire à l'équité des procès de personnes accusées d'être impliquées dans la criminalité organisée ou dans des activités terroristes, les tribunaux acceptant de plus en plus souvent de prononcer une condamnation sur la base d'éléments de preuve secrets ou émanant de témoins anonymes.[5]

4. Cadre juridique

Le cadre juridique déterminant le droit à la vie privée dans le contexte de la lutte contre le terrorisme est complexe ; il se décline en plusieurs instruments distincts aux niveaux national et international.

Au niveau le plus général, la protection des données repose sur l'article 8 de la Convention européenne des droits de l'homme.[6] Ces dernières années, la Cour européenne des droits de l'homme a largement reconnu les principes de protection des données garantis par cet article, notamment dans les affaires *Peck c. Royaume-Uni* (vidéosurveillance), *Amann c. Suisse* (écoutes téléphoniques) et *Rotaru c. Roumanie* (dossiers des services secrets).[7] On pourra également se reporter à l'affaire récente *Copland c. Royaume-Uni* (sur le fait que les fondements juridiques en matière de traitement de données à caractère personnel doivent, pour être acceptables, avoir valeur de loi au sens de la Convention européenne des droits de l'homme).[8]

Cela étant, la protection des données est de plus en plus considérée comme un droit *sui generis*, notamment par la Charte des Droits fondamentaux de l'Union européenne, qui contient une disposition spéciale sur la protection des données à caractère personnel (article 8).[9] Les instruments de protection suivants ont été spécialement élaborés au niveau européen :

- la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel ;[10]

- la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;[11]

---

[4] Voir par exemple *New study highlights discrimination in use of anti-terror laws*, communiqué de presse relatif à une étude de l'Institute for Race Relations britannique (organe gouvernemental s'intéressant aux relations entre les races), publiée le 2 septembre 2004. Ce communiqué est consultable à l'adresse suivante : http://www.irr.org.uk/2004/september/ak000004.html; l'étude in extenso peut être téléchargée à l'adresse suivante : http://www.irr.org.uk/pdf/terror_arrests_study.pdf (en anglais).

[5] Voir John Vervaele, *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?* Dans la revue *Utrecht Law Review*, Volume 1, Issue 1 (septembre 2005), http://www.utrechtlawreview.org/ (en anglais)

[6] Convention européenne des droits de l'homme, 4 novembre 1950, STE n° 5. Article 8.1 – Droit au respect de la vie privée et familiale **-** Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

[7] Arrêt *Peck c. Royaume-Uni*

[8] Arrêt *Copland c. Royaume-Uni* du 3 avril 2007.

[9] Charte des Droits fondamentaux de l'Union européenne, article 7 - Respect de la vie privée et familiale - Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ; article 8 - Protection des données à caractère personnel - 1. Toute personne a droit à la protection des données à caractère personnel la concernant. - 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. - 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

[10] Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n° 108, du 28 janvier 1981 ; Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données, STE n° 181, du 8 novembre 2001. Les deux textes sont disponibles in extenso à l'adresse suivante : http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/. Des amendements à la convention ont été rédigés et adoptés par le Comité des Ministres pour permettre aux Communautés européennes (et non à l'Union européenne) d'adhérer à la convention : ces amendements sont accessibles sur la même page web. Ils ne sont pas encore entrés en vigueur et les Communautés européennes ne sont pas encore parties à la convention.

[11] JO n° L 281 du 23/11/1995, p. 31 : http://ec.europa.eu/justice_home/fsj/privacy/law/index_fr.htm. Les exigences de la directive sont décrites en détail dans l'ouvrage de Douwe Korff intitulé *Data Protection Law in Practice in the European Union*, Bruxelles/New York, 2005 (en anglais).

- la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques »).[12]

  [Remarque : 1) cette directive revêt un caractère subsidiaire par rapport à la directive 95/46/CE ; 2) elle a été modifiée pour permettre la conservation de données de communication par les fournisseurs d'accès obligatoire aux fins d'application de la loi.][13]

En complément, ont été adoptés plusieurs textes réglementaires et d'orientation portant plus particulièrement sur le traitement des données à caractère personnel à des fins répressives, par exemple la recommandation du Conseil de l'Europe n° R (87) 15 du Comité des Ministres aux Etats membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (1987).[14] Cette recommandation est devenue la norme en la matière : plusieurs instruments européens de coopération policière y font expressément référence, notamment les traités de Schengen et Europol et les règlements connexes, ainsi que des recommandations de l'Assemblée parlementaire et du Comité des Ministres du Conseil de l'Europe, et du Parlement européen.

A l'instar de la Cour de Strasbourg, la Cour européenne de Justice de Luxembourg a opté pour une application très stricte des principes de protection des données (fondée, en ce qui concerne la CEJ, à la fois sur la Convention européenne des droits de l'homme telle que reprise dans les principes généraux du droit communautaire et sur les directives ci-dessus ; voir notamment les affaires *Österreichischer Rundfunk c. Autriche* et *Lindqvist c. Suède*).[15] Il ressort sans ambiguïté de ces arrêts, et c'est important, que la Cour européenne de Justice considère la protection des donnée comme une question constitutionnelle, fondamentale : les dispositions de la principale directive sur la protection des données doivent être interprétées comme des principes constitutionnels fondamentaux des droits de l'homme et appliqués conformément à la jurisprudence de la Cour européenne des droits de l'homme. Plus précisément, la CEJ a clairement approuvé et fait sienne la manière d'envisager les droits de l'homme caractéristique de la Cour de Strasbourg – une conception qu'elle a adoptée, en particulier pour examiner les affaires touchant à la directive cadre.

On retrouve les grandes règles ci-après – qui découlent des arrêts de la Cour européenne des droits de l'homme – dans la jurisprudence de la CEJ et la Recommandation n° R(87)15 :

1. Toute opération de collecte, de stockage, d'utilisation, d'analyse ou de divulgation/d'échange de données à caractère personnel à des fins répressives ou antiterroristes doit reposer sur une base légale. Une vague base légale générale ne suffit pas;[16] au contraire :

2. Ces opérations doivent être fondées sur les règles légales spécifiques relatives à chaque type d'opération spécifique ; ces règles doivent être contraignantes et fixer des limites appropriées aux pouvoirs conférés aux autorités telles que :

---

[12] La Directive 2002/58/CE a remplacé une directive antérieure, la Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (« directive RNIS ») ; les deux peuvent être consultées à l'adresse suivante : http://ec.europa.eu/justice_home/fsj/privacy/law/index_fr.htm.

[13] Modification par 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, JO n° L 105 du 13.04.2006 p. 54, consultable sur : http://ec.europa.eu/justice_home/fsj/privacy/law/index_fr.htm.

[14] http://www.coe.int/t/f/affaires_juridiques/coopération_juridique/protection_des_données/documents/instruments_juridiques_internationaux/Rec(87)15_FR.pdf

[15] *Österreichischer Rundfunk c. Autriche*, affaires jointes C-465/00 (*Rechnungshof c. ÖRF et autres*), C-138/01 et C-139/01 (respectivement, *Christa Neukomm* et *Lauermann c. ÖRF*) (demandes de décision préjudicielle du *Verfassungsgerichtshof* et de l'*Oberster Gerichtshof*), conclusions de l'avocat général, M. Tizzano, du 14 novembre 2002 et arrêt du 20 mai 2003 ; *Lindqvist c. Suède*, affaire C-101/01 *Bodil Lindqvist c. Åklagarkammaren i Jönköping* (demande de décision préjudicielle du Göta hovrätt), conclusions de l'avocat général, M. Tizzano, du 19 septembre 2002 et arrêt du 6 novembre 2003. Ces arrêts sont résumés dans l'article de Douwe Korff, *Paper No. 4: The Legal Framework*, publié dans *Privacy & Law Enforcement* (note 6, ci-dessus), Ian Brown & Douwe Korff, pages 34-44.

[16] Dans l'arrêt *Copland c. Royaume-Uni* (voir note 8 ci-dessus), la Cour a estimé que l'existence dans le droit anglais d'une disposition vague d'habilitation ne suffisait pas et qu'une telle disposition, même si elle était considérée comme satisfaisante par les tribunaux anglais, ne s'apparentait pas à une « loi » au sens de la Convention européenne des droits de l'homme.

- une description précise du type d'informations susceptibles d'être enregistrées ;
- une description précise des catégories de personnes pouvant faire l'objet de mesures de surveillance supposant la collecte et la conservation d'informations ;[17]
- une description précise des circonstances dans lesquelles de telles mesures peuvent être prises ;
- une procédure clairement établie de demande d'autorisation pour appliquer ces mesures ;
- des limites relatives au stockage d'informations anciennes et à la durée de conservation de nouvelles informations ;
- des dispositions détaillées et explicites sur :
  - les motifs de création des dossiers ;
  - la procédure à suivre [pour créer les dossiers ou y accéder] ;
  - les personnes autorisées à consulter les dossiers ;
  - la nature des dossiers ;
  - les possibilités d'utilisation des informations contenues dans les dossiers.

Il découle de ce qui précède que :

1) la collecte de données sur les personnes associées ou les contacts (c'est-à-dire des personnes qui ne sont pas soupçonnées d'avoir participé à la commission d'une infraction particulière ou de constituer une menace), la collecte d'informations par des dispositifs d'intrusion ou des moyens secrets (écoutes téléphoniques, interception de messages électroniques, dispositifs d'écoute, informateurs, agents de renseignement), le recours à des techniques de profilage et, bien sûr, les mesures de police préventive en général doivent répondre à des critères particulièrement stricts de nécessité et de proportionnalité (toutes ces mesures doivent aussi être entourées de garanties extrêmement solides : voir ci-après) ;
2) il convient de distinguer clairement d'une part, les données factuelles des données fondées sur le renseignement et, d'autre part, les différentes catégories de personnes visées (personnes officiellement mises en examen, suspects, complices, relations fortuites, témoins, victimes, etc.) ;
3) la nature des informations et renseignements provenant d'entités privées telles que des entreprises ou des sociétés de renseignement commercial exige des garanties supplémentaires : il faut vérifier, entre autres, l'exactitude de ces données qui revêtent un caractère personnel et ont été collectées à des fins commerciales dans un contexte commercial ;
(4) l'accès aux données ne devrait être autorisé qu'au cas par cas, à des fins spécifiées et sous contrôle judiciaire dans les Etats membres.

3. Ces règles peuvent prendre la forme d'une réglementation subsidiaire mais, pour pouvoir prétendre au statut de loi aux termes de la convention, elles doivent être rendues publiques.

4. Pour répondre au principe essentiel selon lequel les objectifs poursuivis doivent être définis et limités, il faut respecter les règles suivantes :

   - il importe d'être aussi précis que possible; il ne suffit pas d'indiquer que le traitement de données envisagé entre dans le cadre du travail de police ni même d'une tâche spécifique (enquête et poursuites pénales, réaction à une menace immédiate ou encore – plus discutablement – prévention) ;
   - les données à caractère personnel collectées pour un besoin de police particulier (parer une menace, par exemple) ne peuvent être utilisées à d'autres fins (enquêter sur une infraction, par exemple) que si elles auraient pu être recueillies dans ce second but de manière indépendante ;
   - les données à caractère personnel ne doivent jamais être collectées par la police ou d'autres services chargés de l'application de la loi « au cas où ».

[17] Il est à noter que la Cour considère clairement la collecte et la conservation d'informations dans des dossiers de renseignement comme des « mesures de surveillance » en tant que telles. La qualification ne repose pas sur les moyens employés : la « surveillance » ne se limite pas aux opérations menées avec des moyens techniques secrets. Elle peut être exercée sur des individus moyennant la collecte d'informations par des méthodes ouvertes ou auprès de sources publiques (pétitions contre la guerre en Iraq, coupures de presse, réalisation ouverte de photographies ou de films dans des manifestations, par exemple).

5. « La collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée. La collecte de données concernant ces facteurs ne peut être effectuée que si elle est absolument nécessaire pour les besoins d'une enquête déterminée. » (principe 2.4 de la Recommandation n° R(87)15)

6. Concernant le premier pilier, la Directive 95/46/CE précise que toute personne soumise à une décision automatisée doit (au moins) avoir le droit de connaître la logique qui sous-tend cette décision, et que des mesures doivent être prises pour garantir son intérêt légitime. La portée et l'application de ce principe demeurent assez vagues, y compris dans le cadre du premier pilier. Cependant, le principe sous-jacent – selon lequel tout traitement de ce type opéré sans garanties strictes constituerait une violation de l'identité, de la dignité ou de la personnalité de l'individu concerné – doit certainement aussi être appliqué dans le cadre du troisième pilier. Il est clair que cela a des conséquences pour le profilage des terroristes présumés évoqué ci-dessus.

7. Il convient en outre de prévoir de solides « garanties établies par la loi et qui sont [effectives et] applicables au contrôle des activités des services concernés ». Ce contrôle doit normalement être assuré par le pouvoir judiciaire. Si tel n'est pas le cas, il devrait exister des mécanismes de remplacement particulièrement puissants tels qu'un contrôle parlementaire.[18] Cette dernière exigence procédurale (le contrôle) est l'un des critères d'évaluation de la qualité de la règle légale en question. L'existence de telles procédures est également essentielle pour évaluer la conformité à l'article 13 de la Convention européenne des droits de l'homme (droit à un recours effectif devant une instance nationale). La Cour européenne des droits de l'homme a également confirmé qu'une voie de recours devrait être accessible à quiconque se prétend victime de manière plausible d'une violation d'un droit garanti par la convention : il n'est pas nécessaire de montrer que la violation est bien réelle – ce qui, dans le cas d'une surveillance secrète, mettrait les personnes concernées dans une position impossible.

5. Le contexte européen

Les questions traitées dans le présent document s'inscrivent dans un cadre international et institutionnel complexe. En effet, elles sont liées à des activités menées par le Conseil de sécurité des Nations Unies, l'Organisation pour la sécurité et la coopération en Europe (OSCE), divers organes politiques et normatifs du Conseil de l'Europe (l'Assemblée parlementaire et le Comité des Ministres, par exemple), des organes de l'Union européenne (le Parlement européen, la Commission européenne et le Conseil européen, qui joue un rôle prépondérant), l'Otan et de grands pays, en particulier les Etats-Unis. Selon l'acteur (ou l'organe), ces activités relèvent du domaine politique ou diplomatique ou concernent la police, les services de renseignement ou l'armée.

La lutte contre le terrorisme est considérée de plus en plus comme un problème mondial qui nécessite une réponse mondiale elle aussi. D'une part, le socle juridique de la protection des droits de l'homme et de la protection des données a été établi au niveau européen. D'autre part, les politiques qui risquent de menacer ces normes européennes, telles que les politiques de lutte contre le terrorisme, sont également élaborées au niveau européen. En conséquence, la partie qui suit porte sur le rôle de l'Union européenne dans la lutte contre le terrorisme et la criminalité organisée et examine comment cette action de l'Union rejoint les questions de protection des données.

5.1 Promotion des technologies de l'information

L'Union européenne encourage fortement l'utilisation des nouvelles technologies de l'information dans des domaines comme l'administration (« e-gouvernement »), la santé (« e-santé »), l'inclusion (« e-inclusion ») ou l'éducation (« e-learning »), ainsi que la prestation de services en ligne paneuropéens

18 Voir les arrêts *Klass et autres c. Allemagne* et *Kopp c. Suisse* de la Cour européenne des droits de l'homme, auxquels renvoie expressément sur ce point l'arrêt *Rotaru c. Roumanie*.

par le secteur privé (qui se mondialise de plus en plus). On observe que l'utilisation de l'informatique est aussi encouragée en matière répressive ; à cet égard, la lutte contre le terrorisme est un puissant catalyseur.

La Commission européenne estime que la gestion de l'identification électronique (e-ID) figure parmi les « outils clés essentiels » de l'administration en ligne :[19]

> Les cartes d'identité biométriques et l'e-ID pour les services publics ont des finalités nettement différentes : les cartes d'identité nationales ont une fonction de sécurité publique, notamment en facilitant le contrôle intégré des frontières et en contribuant à la lutte antiterroriste, tandis que l'identification électronique pour les services publics est destinée à en faciliter l'accès et à offrir des services personnalisés et plus performants.[20]

Du point de vue de la protection des données, cette différence de finalité devrait conduire impérativement à faire la distinction entre ce qui concerne les cartes d'identité et ce qui concerne l'e-ID, et à bien séparer les bases de données utilisées par ces deux outils.

5.2 Systèmes et bases de données de l'UE pour l'application de la loi

Europol

Organisation européenne de mise en application de la loi, Europol traite des renseignements relatifs aux activités criminelles. Son objectif est d'améliorer l'efficacité des services compétents des Etats membres et leur coopération en ce qui concerne la prévention et la répression du terrorisme et des formes graves de criminalité internationale organisée. Europol a pour mission de contribuer au volet « application de la loi » de l'action menée par l'Union européenne contre la criminalité organisée et le terrorisme, en concentrant ses efforts sur les organisations criminelles. Le Conseil européen a souligné l'importance du « renforcement des capacités opérationnelles d'Europol ».[21]

Eurojust

Créé en 2002, Eurojust est le premier réseau international permanent qui ait été créé dans le monde entre les instances responsables des enquêtes et des poursuites pénales.[22] Eurojust stimule et améliore la coopération entre les autorités compétentes des Etats membres, notamment en facilitant la mise en œuvre de l'entraide judiciaire internationale et l'exécution des demandes d'extradition. En outre, le réseau apporte un soutien logistique (traduction, par exemple) dans le cadre de l'organisation de réunions entre des enquêteurs et des procureurs de différents Etats ; ces réunions portent sur des affaires précises ou sur des thèmes plus généraux (questions stratégiques ou types de criminalité spécifiques). Eurojust se consacre de plus en plus aux affaires de terrorisme et souhaiterait étendre ses activités dans ce domaine.[23]

Eurodac

Eurodac est un système qui permet de comparer les empreintes digitales des demandeurs d'asile et des personnes soupçonnées d'être entrées illégalement sur le territoire de l'Union européenne ; il contribue ainsi à l'application effective de la convention de Dublin sur le traitement des demandes d'asile. Du point de vue du thème du présent document, ce qui est le plus préoccupant, c'est que, selon les nouvelles propositions, et notamment selon le nouveau « principe de disponibilité », l'utilisation et les finalités de la base de données d'Eurodac seront étendues à la quasi-totalité des questions relatives à l'application de la loi et à la sécurité publique dans l'UE, dont le terrorisme. Le

[19] Plan d'action i2010 pour l'e-gouvernement. A propos de ce plan, voir : http://europa.eu/scadplus/leg/fr/lvb/l24226j.htm
[20] Idem.
[21] Newsletter du CEPD (contrôleur européen de la protection des données) du 9 juillet 2007. Pour plus de précisions, voir le document COM (2006) 817 (Proposition de décision du Conseil portant création de l'Office européen de police (EUROPOL)) de décembre 2006, qui tend à remplacer la Convention Europol et l'acquis correspondant par une nouvelle décision donnant à Europol des pouvoirs opérationnels.
[22] Alors qu'Eurojust œuvre en matière pénale, il existe aussi un Réseau judiciaire en matière civile et commerciale, qui a été établi en 2001. Voir : http://ec.europa.eu/civiljustice/.
[23] Voir, par exemple, le rapport annuel 2006 d'Eurojust, p. 6. Ce rapport est disponible à l'adresse suivante : http://www.eurojust.europa.eu/press_releases/annual_reports/2006/Annual_Report_2006_FR.pdf.

comité permanent d'experts en droit international de l'immigration et des réfugiés et en droit pénal international (le « Comité Meijers ») s'est fermement opposé à cette extension dans une lettre qui contient en particulier le passage suivant :

> Les mesures et les politiques de l'UE dans le domaine de la liberté, de la sécurité et de la justice ne doivent pas se fonder sur la présomption générale selon laquelle il faut traiter les migrants qui se trouvent sur le territoire de l'UE comme des terroristes présumés. Une telle attitude serait contraire aux principes généraux de non-discrimination et d'égalité qui sous-tendent le droit communautaire. Elle aurait aussi des conséquences dévastatrices pour la situation des migrants et leur future intégration dans la société des Etats membres de l'UE.[24] [traduction de l'anglais]

Le système d'information Schengen (SIS)

A l'origine, le système d'information Schengen (SIS) était un dispositif destiné à réduire les risques liés à l'ouverture des frontières, et il portait sur un ensemble de données limité. Cependant, après une extension qui a abouti à la version « SIS-I+ », la préparation d'un nouveau système, le SIS-II, est maintenant en bonne voie. Le SIS-II devrait avoir « des fonctionnalités plus avancées » et être fondé sur « des technologies de pointe ». Le nouveau système permettra également « la connexion d'autres Etats membres ».[25] Il comportera des listes de toutes les personnes auxquelles il faut refuser l'entrée sur le territoire, ainsi que des listes de personnes « connues » ou « suspectes » en rapport avec la criminalité ou le terrorisme, et une autre liste où figureront les personnes à placer sous surveillance. Il est prévu d'étendre l'accès à ces données à Europol, à Eurojust, aux parquets nationaux et aux services chargés de l'immatriculation des véhicules.

Ainsi que la Chambre des lords britannique l'a fait remarquer, le SIS-II stockera un énorme volume de données sensibles à caractère personnel.[26] Plus généralement, comme la Commission européenne l'a reconnu, le SIS, qui est à l'origine un système d'information, se transformera, du fait de ses nouvelles fonctions, en un système d'information et d'enquête.[27] Or, la Chambre des lords a aussi souligné que le régime de protection des données applicable au SIS-II était inutilement complexe.

Système d'information sur les visas (VIS)

Le système d'information sur les visas (VIS), créé en 2004, a été conçu comme un système d'échange de données sur les visas entre les Etats membres. Lors d'une réunion tenue le 7 mars 2005, le Conseil de l'Union européenne a adopté des conclusions selon lesquelles un accès au VIS doit être garanti aux autorités des Etats membres compétentes en matière de sécurité intérieure « afin de remplir pleinement l'objectif d'amélioration de la sécurité intérieure et de la lutte contre le terrorisme ». En juillet 2007, le Conseil européen a appelé à mettre en œuvre rapidement la décision sur l'accès par les autorités répressives (y compris Europol) à la base de données VIS aux fins de la prévention et de la détection des infractions terroristes et aux fins des enquêtes sur ces infractions.[28] Cet accès a été autorisé en vertu d'une décision du Conseil du 23 juin 2008.[29]

---

[24] Cette lettre peut être consultée (en anglais) à l'adresse suivante : http://www.commissie-meijers.nl/assets/commissiemeijers/Commentaren/2007/CM0712-IV%20Comments%20Standing%20Committee%20on%20the%20use%20of%20Eurodac_EC.pdf.

[25] http://europa.eu/scadplus/leg/fr/lvb/l33020.htm, dans la rubrique « Le système d'information de Schengen de deuxième génération (SIS II) ». On y trouve aussi l'explication suivante : « En attendant que le SIS II devienne opérationnel, le Conseil « Justice et affaires intérieures » de décembre 2006 a donné son aval au projet SISone4all (un projet des Etats membres coordonné par le Portugal). Le SISone4all est une solution temporaire ayant pour objet de connecter 9 pays membres UE-2004 à la version existante du SIS I+ (avec quelques adaptations techniques), afin de permettre à ces pays de compléter les évaluations de Schengen aussitôt que possible en vue de la suppression des contrôles aux frontières internes. Les travaux sur SISone4all devraient être terminés avant la fin août 2007. » (Le SIS I+ est déjà une version améliorée du SIS d'origine).

[26] Commission pour l'Union européenne de la Chambre des Lords, neuvième rapport, sur le système d'information Schengen, 20 février 2007 ; ce rapport peut être consulté (en anglais) à l'adresse suivante : http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/49/4902.htm.

[27] Idem.

[28] Newsletter du CEPD du 9 juillet 2007.

[29] Décision 2008/633/JAI du Conseil du 23 juin 2008.

Système d'information douanier (SID)

C'est une base de données relevant des premier et troisième piliers qui vise à aider les autorités douanières et les autres autorités compétentes à prévenir les infractions graves aux législations nationales, à enquêter sur ces infractions et à poursuivre leurs auteurs. Des informations peuvent être enregistrées aux fins d'observation et de compte rendu, de surveillance discrète ou de contrôles spécifiques. Le SID est géré par l'Office européen de lutte anti-fraude (OLAF), en coopération avec la Direction générale Justice et Affaires intérieures de la Commission européenne et la DG Fiscalité et Union douanière.

Bien qu'elles concernent principalement la fraude douanière, les données du SID peuvent aussi avoir un rapport avec le terrorisme : c'est par exemple le cas des données portant sur le blanchiment d'argent, le trafic de drogue ou d'autres pratiques frauduleuses ou infractions douanières « ordinaires » destinées à financer des activités terroristes.

Le traité de Prüm

Le traité de Prüm a été signé le 27 mai 2005 par l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas, l'Autriche et la Belgique. Il couvre une série de questions relevant du domaine de la justice et des affaires intérieures, y compris le libre échange d'informations. Par exemple, les articles 2 à 12 prévoient l'accès mutuel direct des services répressifs des Etats participants à leurs bases de données sur l'ADN, les empreintes digitales et l'immatriculation des véhicules ; ainsi, l'autorité policière compétente d'un Etat membre peut interroger une base de données située dans un autre Etat membre sur la concordance/non-concordance (« hit/no-hit ») des empreintes ou de l'ADN, et en cas de concordance, le fichier concerné est communiqué. En fait, le traité requiert la création, dans les Etats parties, de certaines bases de données, dont une sur l'ADN, et impose aux Etats parties l'obligation de se procurer un échantillon de l'ADN de « certaines personnes » (pas nécessairement suspectes) si cet ADN ne figure pas déjà dans la base de données nationale. La lutte contre le terrorisme est explicitement mentionnée parmi les objectifs du traité.

Par sa décision du 23 juin 2008[30], le Conseil européen a convenu d'intégrer les principales dispositions du traité de Prüm dans le cadre juridique de l'UE, pour permettre de plus larges échanges (entre tous les Etats membres de l'UE) de données biométriques (ADN et empreintes digitales) aux fins de la lutte contre le terrorisme et la criminalité transfrontalière. Tous les Etats membres de l'UE devront donc créer des bases de données ADN.

5.3 Le principe de disponibilité

Dans le « programme de La Haye » de 2004 de l'Union européenne, le « principe de disponibilité » est défini comme suit :[31]

> A compter du 1er janvier 2008, l'échange [d']informations devrait obéir aux conditions énumérées ci-après concernant le principe de disponibilité, selon lequel, dans l'ensemble de l'Union, tout agent des services répressifs d'un Etat membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre Etat membre, l'administration répressive de l'autre Etat membre qui détient ces informations les mettant à sa disposition aux fins indiquées et en tenant compte des exigences des enquêtes en cours dans cet autre Etat.
>
> […] Les méthodes utilisées pour échanger les informations devraient exploiter pleinement les nouvelles technologies et être adaptées à chaque type d'information, s'il y a lieu, par le biais d'un accès réciproque aux banques de données nationales, de leur interopérabilité ou de l'accès direct (en ligne), y compris pour Europol, aux bases de données centrales dont dispose déjà l'UE, telles que le SIS.

[30] Décision 2008/615/JAI du Conseil du 23 juin 2008 et Décision 2008/616/JAI datée du même jour.
[31] Le programme de La Haye : renforcer la liberté, la sécurité et la justice dans l'Union européenne, adopté par le Conseil européen le 4 novembre 2004 (document dont la définition est extraite). Voir aussi le Plan d'action du Conseil et de la Commission mettant en œuvre le programme de La Haye visant à renforcer la liberté, la sécurité et la justice au sein de l'Union européenne.

En vertu de ce principe, les services répressifs des Etats membres de l'UE ont en pratique un accès plein et entier à toutes les données figurant dans toutes les bases de données nationales et européennes. Le but est notamment de permettre cet échange de données et cette liberté d'accès en levant tous les « obstacles » habituels contenus dans les instruments traditionnels relatifs à la coopération transnationale entre les services répressifs ; parmi ces instruments figurent la Convention européenne d'entraide judiciaire en matière pénale (traité du Conseil de l'Europe, 1959, STE n° 030) et ses deux protocoles additionnels, ainsi que la Convention de 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne (qui s'inspire de la convention du Conseil de l'Europe) et son protocole de 2001, entrés en vigueur tous deux en 2005. Les procédures prévues par ces traités prennent du temps et, surtout, nécessitent des demandes officielles d'informations précises et, souvent, l'autorisation d'une instance judiciaire.

Or, ces « obstacles » constituent en fait dans bien des cas des garanties fondamentales pour l'individu. Les autorités européennes de protection des données ont mis en garde contre le danger de lever tous ces obstacles, dans une déclaration adoptée lors de la réunion qu'elles ont tenue à Chypre en mai 2007 :

> Etant donné que la disponibilité des informations est présentée de plus en plus comme un postulat nécessaire de l'amélioration de la lutte contre la criminalité, et que le principe de disponibilité est appliqué au niveau national et entre les Etats membres, l'absence, dans l'Union, d'un régime de protection des données harmonisé et de haut niveau crée une situation dans laquelle le droit fondamental à la protection des données à caractère personnel ne fait plus l'objet de garanties suffisantes. [traduction de l'anglais]

Les autorités de protection des données ont suggéré d'élaborer un ensemble complet de dispositions pour encadrer l'application du principe de disponibilité, et formulé des lignes directrices à cet égard. La mise en œuvre de celles-ci permettrait de limiter considérablement le recours au principe de disponibilité et d'apporter des garanties.[32]

Si la proposition d'adoption officielle du principe de disponibilité n'a pas été retenue, ce principe reste néanmoins souvent le fondement des échanges de données, par exemple dans le traité de Prüm.

5.4 La proposition de décision-cadre du Conseil de l'UE relative à la protection des données à caractère personnel

La proposition de décision-cadre du Conseil de l'UE relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale vise à garantir un niveau élevé de protection des données en ce qui concerne l'ensemble du troisième pilier. Cette proposition a cependant été sévèrement critiquée par le Parlement européen, le contrôleur européen de la protection des données (CEPD) et toutes les autorités européennes de protection des données, ainsi que par la société civile et plusieurs groupes de défense des droits de l'homme. Ce qui est généralement reproché à la proposition (dans sa version actuelle), c'est d'encourager une tendance à un nivellement vers le bas de la protection des données dans le cadre du troisième pilier de l'UE. Selon les critiques, la proposition actuelle reste en deçà des normes européennes déjà établies, en particulier : la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), la recommandation, inspirée de cette convention, qui vise à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (la Recommandation n° R (87) 15, déjà mentionnée), et une disposition plus large et plus fondamentale, l'article 8 de la Convention européenne des droits de l'homme. La décision proposée semble également créer des failles, qui permettraient d'échapper aux règles rigoureuses de protection des données en vigueur dans certains pays de l'UE en faisant passer les données par d'autres pays, où les restrictions sont moins sévères. Enfin, il est prévu d'exclure du champ d'application de la décision les activités des services secrets et de la police liées à la sécurité nationale ; dans le cadre de ces activités, il n'existerait donc aucune garantie effective en matière de protection des données.

[32] http://www.cnpd.pt/bin/relacoes/declaration.pdf (en anglais)

5.5 Données des dossiers passagers (« Passenger Name Record », PNR)

Les données des dossiers passagers (PNR) concernent les déplacements, habituellement par voie aérienne, et comprennent les données du passeport, le nom, l'adresse, les numéros de téléphone, l'agence de voyage, le numéro de la carte de crédit, l'historique des modifications du plan de vol, les préférences de siège et d'autres informations. Les transporteurs aériens enregistrent déjà les données des dossiers passagers pour leur propre usage commercial, mais seuls quelques Etats membres ont adopté une législation visant à instaurer des mécanismes pour contraindre les transporteurs aériens à fournir les données PNR et permettre l'analyse de ces données par les autorités compétentes.

Les transporteurs aériens communiquent déjà certains types de données aux autorités des Etats membres de l'UE, à savoir les informations préalables sur les voyageurs (« Advanced Passenger Information » (API))[33], qui sont utilisées principalement aux fins du contrôle des frontières et de la lutte contre l'immigration illégale. Les PNR contiennent davantage d'éléments que les API, qui sont simplement des données officielles figurant sur les passeports. Selon la Commission européenne, les PNR présentent un plus grand intérêt dans la lutte contre le terrorisme car « [c]es éléments sont très importants pour procéder à des évaluations de risques des personnes, pour obtenir des informations et pour établir des liens entre des personnes connues et des personnes inconnues ».[34]

Des accords pour la transmission de données PNR dans le contexte de la lutte contre le terrorisme et la criminalité transnationale organisée ont été conclus par l'UE avec les Etats-Unis[35], le Canada et, dernièrement, l'Australie[36].

En 2004, le Conseil européen a invité la Commission à soumettre une proposition en vue d'une approche commune de l'UE dans l'utilisation des données passagers à des fins répressives. La Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives a été présentée par la Commission en novembre 2007, après une période de consultation des acteurs concernés.

Plusieurs réserves importantes ont été émises sur cette proposition par le groupe de travail « Article 29 »[37] et par la société civile. Dans son avis sur le projet de proposition, le contrôleur européen de la protection des données, quant à lui, juge « évident […] que les mesures envisagées portent atteinte à la vie privée. En revanche, leur utilité est loin d'être démontrée. » [38] Le 28 octobre 2008, l'Agence des droits fondamentaux de l'Union européenne a elle aussi publié un avis sur la proposition, dans lequel elle examine de manière critique plusieurs dispositions de la proposition ; l'Agence s'interroge notamment sur l'imprécision de certaines formulations, le caractère nécessaire et proportionné des mesures envisagées et le risque d'établissement discriminatoire de profils.[39] Selon l'Agence, il n'est pas toujours possible de garantir le respect des normes européennes relatives à la protection des données lorsque des données à caractère personnel sont traitées hors de l'UE ; en conséquence, le transfert de données PNR vers des pays tiers crée un risque d'atteintes graves aux droits fondamentaux.

---

[33] En vertu de la Directive 2004/82/CE du Conseil.
[34] Proposition COM(2007)654 final.
[35] Accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), Journal officiel n° L 204 du 04/08/2007 p. 0016 - 0025).
[36] Accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers (Journal officiel n° L 82 du 21/03/2006, p. 15 – 19). Accord entre l'Union européenne et l'Australie : Journal officiel du 08/08/2008.
[37] Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives, présentée par la Commission le 6 novembre 2007, adopté le 5 décembre 2007 par le groupe de travail « Article 29 » et adopté le 18 décembre 2007 par le groupe de travail sur la police et la justice, WP 145, WPPJ 01/07.
[38] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_FR.pdf
[39] http://fra.europa.eu/fra/material/pub/discussion/FRA_opinion_PNR_en.pdf (en anglais).

5.6 Profilage

Le profilage est une méthode de plus en plus utilisée, non seulement par des forces de police et/ou des services secrets nationaux isolés, mais aussi dans le cadre de la coopération internationale.

De nombreux éléments pourraient être inclus dans la présentation des profils terroristes : nationalité, document de voyage, mode et moyen de transport, âge, sexe, signes physiques particuliers (par exemple, cicatrices de blessures provoquées par des armes ou des explosifs), éducation, identité d'emprunt, utilisation de techniques de contre-enquête et de contre-interrogatoire, résidences, méthodes de communication, lieu de naissance, caractéristiques psychosociologiques, situation familiale, compétences en technologies de pointe, compétences en matière de maniement d'armes non conventionnelles (NRBC) et participation à une formation paramilitaire ou aéronautique ou à une autre formation technique spécialisée. Selon l'ONG « Privacy International », les services répressifs pourraient ensuite consulter les bases de données nationales dans l'espoir d'y trouver des éléments équivalents et de mettre ainsi la main sur des terroristes présumés.[40]

Ce « profilage fondé sur le renseignement » est souvent présenté par les autorités comme une technique plus acceptable d'une certaine manière qu'un profilage purement discriminatoire (profilage racial/ethnique). En réalité, il n'y a peut-être guère de différence : cibler des personnes parce qu'elles correspondent à un certain stéréotype (le jeune musulman pratiquant qui, à un moment ou un autre, s'est rendu au Pakistan, par exemple), c'est bel et bien faire du profilage ethnique, racial et religieux.[41]

Dans son avis sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives (28 octobre 2008), l'Agence des droits fondamentaux se montre critique à l'égard du recours au profilage dans le contexte des données PNR.

6. Evaluation

Les Etats sont soumis à l'obligation positive de protéger la vie de leurs citoyens (*Osman c. Royaume-Uni*).[42] Les autorités sont tenues de faire tout ce que l'on peut raisonnablement attendre d'elles pour empêcher la matérialisation d'un risque certain et immédiat pour la vie, dont elles avaient ou auraient dû avoir connaissance. En ce sens, le droit à la sécurité est « codifié » depuis longtemps en tant que droit fondamental dans la jurisprudence de la Cour européenne des droits de l'homme. Cette obligation vaut également dans les situations de danger de mort résultant d'une menace terroriste. En effet, le préambule des Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme adoptées par le Comité des Ministres du Conseil de l'Europe le 11 juillet 2002 fait référence au « devoir impératif des Etats de protéger les populations contre d'éventuels actes terroristes ».[43] Une disposition similaire figure dans les Lignes directrices sur la protection des victimes d'actes terroristes, adoptées par le Comité des Ministres le 2 mars 2005.[44]

Toutefois, en l'affaire *Osman*, la Cour a aussi souligné « la nécessité de s'assurer que la police exerce son pouvoir de juguler et de prévenir la criminalité en respectant pleinement les voies légales et autres garanties qui limitent légitimement l'étendue de ses actes d'investigations criminelles et de traduction des délinquants en justice, y compris les garanties figurant aux articles 5 et 8 de la Convention ». Les Etats ont donc la difficile mission de trouver un équilibre entre des intérêts

[40] Rapport de « Privacy International » sur la discrimination et les politiques antiterroristes en Europe, 20 septembre 2005 ; ce rapport peut être consulté (en anglais) à l'adresse suivante : http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-360509 (voir la rubrique 2.2, intitulée « Subtle Interventions and Surveillance »).

[41] Voir aussi la Recommandation de politique générale n° 11 sur la lutte contre le racisme et la discrimination raciale dans les activités de la police, Commission européenne contre le racisme et l'intolérance (ECRI), 29 juin 2007, CRI(2007)39.

[42] Arrêt du 28 octobre 1998.

[43] Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme, adoptées par le Comité des Ministres le 11 juillet 2002 lors de la 804e réunion des Délégués des Ministres.

[44] Lignes directrices sur la protection des victimes d'actes terroristes, adoptées par le Comité des Ministres le 2 mars 2005, lors de la 917e réunion des Délégués des Ministres.
Voir aussi : Thomas Hammarberg, « Give victims of terrorism sustained compensation and support », discours tenu à la 27e Conférence des Ministres européens de la Justice, « La place, les droits et l'aide aux victimes », Erevan, Arménie, 12-13 octobre 2006, CommDH/Speech(2006)19 (en anglais).

concurrents liés aux droits de l'homme : d'une part, ils doivent protéger leur population contre les menaces terroristes, et, d'autre part, ils doivent garantir les droits fondamentaux des individus, y compris des personnes soupçonnées ou reconnues coupables d'activités terroristes.

Les nouvelles technologies font peser de nouvelles menaces sur l'individu dans la société de l'information. On assiste à un développement considérable de la surveillance directe, par le biais de la vidéosurveillance, des systèmes de reconnaissance des plaques d'immatriculation, etc. La surveillance des personnes par les données (« *dataveillance* ») est aussi en plein essor : elle consiste à suivre les pistes laissées sous forme de données par les personnes lors de nombreuses transactions nécessitant un accès à des bases de données (voir la description faite plus haut). En outre, ce sont de plus en plus souvent les ordinateurs qui déterminent qui « cibler », sur la base de profils informatiques qui sont en réalité impossibles à contester.

Une autre tendance générale consiste à recourir au droit administratif, et aux sanctions administratives, à l'encontre des « fauteurs de troubles », selon des méthodes qui permettent de contourner le droit pénal et ne sont donc pas soumises aux garanties du système de justice pénale, ou qui modifient la loi (normes en matière de preuve ou règles sur l'admissibilité des modes de preuve, par exemple) d'une manière qui porte gravement atteinte aux droits de la personne.

Les politiques antiterroristes et les dispositions connexes accentuent nettement ces tendances préexistantes : nombre de mesures sont instaurées, et acceptées, en vertu de la nécessité de lutter contre la « criminalité organisée » et le « terrorisme » (ces deux termes étant eux-mêmes mal définis). Ces mesures sont souvent adoptées trop facilement, prétendument à titre provisoire ou sous forme de mesures « d'urgence », mais, une fois instaurées, elles deviennent permanentes et s'intègrent dans la législation générale. Or, il est difficile d'introduire dans cette législation des dispositions prévoyant une limitation de leur application dans le temps.

L'utilisation de certaines technologies dans la lutte contre le terrorisme peut aussi donner lieu à des mesures (y compris de nature administrative) qui sanctionnent de nombreux civils innocents et portent atteinte à leur vie privée, sans réussir pour autant à mettre les véritables terroristes hors d'état de nuire. Qui plus est, le profilage informatique risque d'entraîner une discrimination à l'encontre de groupes minoritaires. Le profilage peut avoir des effets dévastateurs pour une personne : elle risque d'être espionnée, harcelée et privée de toute possibilité de voyager, d'occuper un emploi ou un poste de chercheur, voire d'être arrêtée. Le profilage entrave aussi les processus démocratiques.

Par ailleurs, toute mesure prise en vertu du principe de disponibilité doit être proportionnée et respecter les droits fondamentaux de la personne.

Les activités qui consistent à cibler des criminels ou des terroristes « éventuels » ou à établir des profils et qui ne tiennent aucun compte du principe de limitation de la finalité aboutissent toutes à un mélange de tous les types de données, provenant de toutes les catégories de sources publiques et privées : données factuelles ou fondées sur le renseignement, qui concernent des suspects, des témoins, des « contacts », voire des victimes. Ces méthodes empêchent de vérifier la fiabilité des données contenues dans cet amalgame. De plus (et c'est une conséquence inévitable), elles privent les personnes (durement) touchées par ces activités de tout recours effectif.

7. Conclusions

L'instauration rapide de la société de la surveillance résulte en partie des progrès de la technologie et de l'évolution sociale mais les mesures prises pour combattre le terrorisme ne font que renforcer cette tendance.

Dans le contexte actuel de lutte antiterroriste, des personnes risquent d'être soupçonnées d'extrémisme ou d'opposition à l'ordre juridique constitutionnel, même si elles n'ont pas (encore) commis d'infraction pénale (et encore moins d'acte terroriste).

En outre, on utilise de plus en plus des profils informatiques pour sélectionner les « cibles ». Même si les méthodes employées peuvent permettre d'arrêter quelques suspects, il y aura toujours un taux d'échec inacceptable en matière d'identification des véritables terroristes (faux négatifs), doublé d'un

taux tout aussi inacceptable de faux positifs qui se traduisent pour un très grand nombre de personnes injustement soupçonnées par une surveillance, un harcèlement ou des discriminations quand ce n'est pas une arrestation ou pire. On sacrifie la liberté sans gagner en sécurité.

De plus, des mesures administratives, non pénales mais effectivement répressives, sont prises à l'encontre d'extrémistes présumés ou d'« ennemis publics » d'un nouveau type. Ces personnes sont ainsi privées des garanties fondamentales à la fois par les mesures spécifiques prises contre elles à titre individuel et par les discriminations dont elles font l'objet en tant que groupe. Cela marginalise les groupes en question et, au bout du compte, compromet la sécurité.

Dans ce processus, nous sommes tous de plus en plus surveillés et des données sur toutes nos activités, en ligne ou dans le monde réel, sont enregistrées. Cette surveillance généralisée pose de graves problèmes démocratiques que ne résout pas l'affirmation sans cesse réitérée selon laquelle ceux qui n'ont rien à cacher n'ont rien à craindre.

La réponse à cette évolution devrait être la réaffirmation des grands principes de la primauté du droit consacrés, notamment, par la Convention européenne des droits de l'homme, et développés dans la jurisprudence de la Cour européenne des droits de l'homme et de la Cour européenne de Justice, ainsi que dans les instruments juridiques européens directement ou indirectement inspirés de la Convention et de cette jurisprudence, y compris la Recommandation toujours primordiale n° R(87)15 du Conseil de l'Europe sur la protection des données dans le secteur de la police.

Les grands principes sont bien établis et indiquent la voie à suivre :

I. La Convention européenne des droits de l'homme dispose que les autorités publiques doivent justifier toute ingérence dans l'exercice d'un droit fondamental inhérente aux mesures décrites dans le présent document. Elles doivent pour cela montrer que l'ingérence :

   - est « prévue par la loi » ;
   - « constitue une mesure qui, dans une société démocratique, est nécessaire
     - à la sécurité nationale, à la sûreté publique, au bien-être économique du pays,
     - à la défense de l'ordre et à la prévention des infractions pénales […]
     - à la protection des droits et libertés d'autrui » ;
   - est proportionnée ;
   - n'est pas discriminatoire.

II. Les principes applicables de protection des données sont également bien précisés dans la Convention STE n° 108 du Conseil de l'Europe, la Recommandation R(87)15 du Comité des Ministres, la principale directive européenne sur la protection des données (Directive 95/46/CE) et la jurisprudence des cours de Strasbourg et de Luxembourg. Ils prévoient notamment que :

   - Tout traitement de données à caractère personnel à des fins répressives et antiterroristes doit reposer sur des règles légales publiques, contraignantes, claires et spécifiques.
   - La collecte de données relatives à des personnes qui ne sont pas soupçonnées d'être impliquées dans une infraction particulière ou de constituer une menace, la collecte d'informations par des dispositifs d'intrusion ou des moyens secrets et le recours aux techniques de profilage doivent répondre à des critères particulièrement stricts de nécessité et de proportionnalité.
   - Il convient de distinguer clairement les données factuelles de celles fondées sur le renseignement et de ne pas mélanger les données portant sur différentes catégories de personnes.

- L'accès aux dossiers de la police et des services secrets devrait n'être autorisé qu'au cas par cas, à des fins spécifiées ; il devrait par ailleurs faire l'objet d'un contrôle judiciaire dans les Etats membres.

- Des limites relatives au stockage d'informations anciennes et à la durée de conservation de nouvelles informations doivent être fixées.

- La collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée.

- Que des organisations publiques ou privées laissent des ordinateurs prendre des décisions concernant des personnes sans intervention humaine est fondamentalement contraire à l'exigence de respect de l'identité humaine et devraient n'être autorisé qu'exceptionnellement dans le cadre de garanties strictes.

- De solides garanties établies par la loi doivent permettre un contrôle approprié et efficace des activités de la police et des services secrets – y compris dans la lutte contre le terrorisme. Ce contrôle devrait être effectué aux niveaux judiciaire et parlementaire. Toutes les opérations de traitement de données à caractère personnel devraient être soumises à un contrôle strict et efficace opéré par des autorités de protection des données indépendantes et impartiales.

III. Dans la lutte contre le terrorisme et la criminalité organisée, ces principes ne devraient pas être abandonnés mais réaffirmés. Tels qu'ils sont conçus actuellement, le profilage et la coopération mise en place par l'Union européenne et fondée sur le principe de disponibilité risquent de porter atteinte aux normes en vigueur. Il conviendrait de réexaminer ces mesures et propositions afin de s'assurer qu'elles sont conformes au droit européen reconnu, notamment à la Convention européenne des droits de l'homme (telle qu'appliquée par la Cour de Strasbourg), à la Convention STE n° 108 et à la Recommandation n° R(87)15 du Conseil de l'Europe, ainsi qu'à la Directive 95/46/CE.