EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

#4229783

La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme

Président Dean Spielmann
Cour européenne des droits de l'homme

Commission nationale pour la protection des données
Luxembourg
Lundi 28 janvier 2013

Monsieur le Ministre,

Mesdames, Messieurs,

C'est avec beaucoup de plaisir que j'ai accepté de participer à cette journée, qui me permet de saluer l'activité essentielle de la Commission nationale pour la protection des données à l'occasion de son 10ème anniversaire. Les Commissions telles que la votre existent dans un certain nombre de pays et elles y jouent un rôle tout à fait essentiel. Ma présence parmi vous témoigne de l'importance que j'y attache personnellement.

Au niveau européen, on sait que le Conseil de l'Europe a été, en quelque sorte, un pionnier en la matière puisque, dès 1973 et 1974, des recommandations furent adoptées dans le domaine de la protection des données et que, surtout, le 28 janvier 1981, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite convention 108, fut ouverte à la signature des États membres du Conseil de l'Europe.

La pierre apportée par la Cour européenne des droits de l'homme est loin d'être négligeable et c'est ce que je vais m'efforcer de vous démontrer dans mon exposé.

Si on remonte au temps lointain de l'élaboration de la Convention européenne des droits de l'homme, force est de constater qu'elle ne contient aucune référence à la nécessité de protéger les données personnelles. Cela n'est guère surprenant : dans l'immédiat après-guerre, les préoccupations dans ce domaine ainsi que les avancées technologiques étaient limitées. Cela explique donc que cette question fût largement ignorée des rédacteurs du texte.

En revanche, la Charte des droits fondamentaux de l'Union européenne, beaucoup plus récente puisque proclamée à Nice en décembre 2000, n'ignore pas ces questions et son article 8, qui s'intitule « Protection des données à caractère personnel », dispose que :

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

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

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

On ne sera cependant pas surpris qu'une Cour telle que la nôtre, qui se veut proche des évolutions et des préoccupations de nos sociétés, se soit, en définitive, rapidement intéressée à ces questions qui sont désormais largement traitées par la jurisprudence.

L'interprétation « évolutive » des différentes exigences de la Convention à laquelle la Commission et la Cour européenne des droits de l'homme se sont livrées, depuis plus de cinquante ans, a permis de prendre en compte l'évolution de nos sociétés telle qu'elle résulte des nouvelles technologies. Le souci de protéger les données personnelles des citoyens a également et naturellement été pris en compte.

A titre liminaire, il importe de rappeler que le traitement et l'utilisation automatisés de données à caractère personnel, s'ils sont récents, correspondent à un phénomène mondial dont les effets sont largement bénéfiques. Nous en sommes les acteurs et les témoins dans tous les actes de notre vie quotidienne. La réservation de billets de train ou d'avion, les demandes de remboursements de frais médicaux, les démarches relatives à l'obtention de documents d'identité sont des exemples non exhaustifs des circonstances très nombreuses dans lesquelles nous sommes conduits à divulguer à autrui, notamment aux administrations, des informations de nature tout à fait privée, voire intime. Toutes ces données sont non seulement collectées, ce qui, en soi, ne soulève pas de difficulté majeure, mais elles peuvent surtout être traitées, croisées, conservées, tout cela sans que nous en soyons même informés. Ceci a été grandement facilité par les progrès de la technologie dont nous sommes les principaux bénéficiaires en raison de l'amélioration que cela amène dans notre vie quotidienne. Cependant, il arrive que nous en soyons les victimes.

Il n'est pas surprenant que les autorités nationales aient très rapidement compris l'usage qui pouvait être fait de ces données personnelles multipliées à l'infini et à partir desquelles un portrait très complet de chacun d'entre nous peut être effectué. Certes, les raisons pour lesquelles les États démocratiques font usage des données personnelles sont principalement liées à la lutte contre le terrorisme et la criminalité, mais également à l'exercice efficace par l'État de ses

fonctions administratives, objectifs auxquels nous ne pouvons que souscrire. Toutefois, il s'agit clairement d'ingérences dans notre vie privée.

C'est à la **collecte des données** que je consacrerai la première partie de mon intervention. Je parlerai, dans un second temps, de **la conservation et de l'exploitation des données**. Puis, j'évoquerai, plus brièvement, la question de **la divulgation des données** et **l'accès** des personnes **aux données** qui les concernent.

Avant d'évoquer la collecte des données à proprement parler, je souhaite rappeler qu'en l'absence de dispositions spécifiques dans la Convention européenne des droits de l'homme, c'est par le biais de l'article 8 et par une extension de son champ d'application que la Cour est intervenue. On sait que l'article 8 contient un premier paragraphe dans lequel est défini le droit protégé, puis un second qui énonce les restrictions qui peuvent être légitimement appliquées au droit. La jurisprudence s'est donc construite en tenant compte de la nécessité de protéger la vie privée des individus, mais aussi de prendre en considération les limitations ou restrictions opposées par les États. La Cour accepte ces ingérences, mais exige que celles-ci soient prévues par la loi (une loi accessible et prévisible dans ses effets) ; qu'elles poursuivent un but légitime ; qu'elles soient nécessaires dans une société démocratique.

La collecte des données

Nous ne cessons, et en pleine connaissance de cause, de communiquer des données qui nous concernent. Toutefois, c'est souvent à notre insu que des données personnelles peuvent être collectées. Un exemple particulièrement flagrant de données collectées sans que l'intéressé en soit conscient concerne les écoutes téléphoniques, pratique fréquemment utilisée par les services de sécurité.

Les arrêts rendus en matière d'écoutes téléphoniques sont nombreux. Parfois, la Cour a d'emblée sanctionné l'absence de légalité de la mesure. Dès l'affaire *Klass c. Allemagne*[1], il fut entendu que les communications téléphoniques étaient protégées par l'article 8 de la Convention et que leur interception par les services de police et de sécurité s'analysait comme une ingérence, laquelle devait être prévue par la loi et nécessaire dans une société démocratique. L'arrêt *Malone c. Royaume-Uni*[2] qui portait également sur l'interception de communications téléphoniques le compléta utilement, dans la mesure où il donna des indications sur la notion de loi au sens de la Convention. Pour être considérée comme compatible avec la Convention, la loi doit être compatible avec la prééminence du droit et le pouvoir d'appréciation de l'exécutif doit être défini avec une netteté suffisante, compte tenu du but légitime poursuivi, pour fournir à l'individu une protection adéquate contre l'arbitraire. C'est précisément l'absence de bases légales qui conduisit la Cour dans l'affaire Malone à conclure à la violation de la Convention. Elle confirmera cette jurisprudence à l'encontre de la France dans les affaires Kruslin et Huvig[3] qui seront d'ailleurs à l'origine de la loi du 10 juillet 1991, relative au secret des correspondances émises par la voie des télécommunications. Par la suite, la Cour continuera d'examiner à chaque fois si la loi, en vertu de laquelle l'autorité publique mémorise les données personnelles, remplit les conditions telles qu'elles résultent de l'arrêt Malone précité.

Parmi les affaires importantes, on peut notamment citer *l'arrêt Amann c. Suisse* du 16 février 2000[4] : il concernait un appel téléphonique passé au requérant depuis une ambassade pour lui commander un appareil dépilatoire qu'il commercialisait. Cet appel fut intercepté par le ministère public, qui fit établir sur le requérant une fiche par les services de renseignements.

[1] Arrêt Klass et autres du 6 septembre 1978.
[2] Arrêt Malone c. Royaume-Uni du 2 août 1984.
[3] Arrêts Kruslin et Huvig c. France du 24 avril 1990.
[4] Arrêt Amann c. Suisse du 16 février 2000.

La Cour parvint à un constat de violation de l'article 8 en raison de l'enregistrement de l'appel téléphonique et car l'établissement de la fiche, comme sa conservation, n'étaient pas « prévus par la loi », le droit suisse étant imprécis quant au pouvoir d'appréciation des autorités dans ce domaine.

En ce qui concerne les écoutes téléphoniques et l'exigence de base légale, on peut citer aussi l'arrêt *P.G et J.H. c. Royaume-Uni*[5] L'affaire concernait l'enregistrement de la voix des requérants – arrêtés car soupçonnés d'être sur le point de commettre un vol – dans les locaux d'un commissariat. La Cour parvint à un constat de violation de l'article 8, car il n'existait à l'époque des faits aucun système légal permettant de réglementer l'usage des dispositifs d'écoute cachés par la police dans ses propres locaux.

On peut également citer les interceptions qui ont lieu dans un autre contexte, celui des établissements pénitentiaires. Dans l'affaire *Wisse c. France*[6], qui concernait le dispositif d'interception des conversations tenues lors des « parloirs » accordés aux proches des requérants détenus dans des maisons d'arrêt, la Cour a conclu à la violation de l'article 8. Elle a estimé, en effet, qu'en ce concerne les enregistrements des conversations tenues dans les parloirs des prisons, le droit français n'indiquait pas avec assez de clarté la possibilité d'ingérence par les autorités dans la vie privée des détenus, ainsi que l'étendue et les modalités d'exercice de leur pouvoir d'appréciation dans ce domaine.

Elle est parvenue à une conclusion analogue dans une affaire *Vetter c. France*[7] particulièrement intéressante. Dans cette affaire, à la suite de la découverte du corps d'une personne abattue par arme à feu, la police judiciaire, qui soupçonnait le requérant d'être l'auteur de cet homicide, sonorisa l'appartement d'une personne chez qui celui-ci se rendait régulièrement. La

[5] Arrêt P.G et J.H. c. Royaume-Uni, du 25 septembre 2001.
[6] Arrêt Wisse c. France, du 20 décembre 2005.
[7] Arrêt Vetter c. France du 31 mai 2005.

Cour a conclu à la violation de l'article 8, car elle a estimé que dans le domaine de la pose de micros, le droit français n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités.

Enfin, on peut citer, mais cette liste est loin d'être exhaustive, l'arrêt *Taylor-Sabori c. Royaume-Uni*[8] qui concernait l'utilisation par la police de messages de bipeur : les messages qui étaient adressés au requérant – accusé d'association de malfaiteurs pour la fourniture de drogues illicites – étaient interceptés au moyen d'un « clone » de son bipeur. La Cour a conclu à la violation de l'article 8, car aucune disposition légale ne réglementait l'interception de messages reçus sur des bipeurs et transmis par l'intermédiaire d'un système de télécommunications privé.

Autre moyen de collecter les données et qui figure parmi les méthodes de lutte contre la criminalité très utilisées dans nos sociétés, les systèmes de vidéosurveillance extrêmement sophistiqués qui se sont considérablement développés ces dernières années. L'article 8 s'applique ici tout naturellement. Dans ce domaine, on peut citer l'arrêt *Peck c. Royaume-Uni*,[9] qui indique dans quelles conditions de telles méthodes peuvent être autorisées et sur lequel je reviendrai un peu plus tard en évoquant la question de la divulgation des données personnelles.

Si la collecte des données ne soulève pas, en soi, de difficulté majeure, la conservation des données personnelles est une question autrement plus délicate.

La conservation des données personnelles

Dans nos sociétés démocratiques, l'existence de services de sécurité et de renseignement est parfaitement légitime. Nous sommes pleinement conscients que, pour défendre l'ordre, prévenir les infractions pénales ou protéger la

[8] Arrêt Taylor-Sabori c. Royaume-Uni du 22 octobre 2002.
[9] Arrêt Peck c. Royaume-Uni du 28 janvier 2003

sécurité nationale, de tels organes conservent les données personnelles qui ont été collectées. Notre Cour ne peut tolérer ce pouvoir de surveillance que sous certaines conditions et toujours avec le souci de sauvegarder les institutions démocratiques.

La Cour apprécie les intérêts en présence et les arguments avancés par les autorités pour justifier la conservation des données. Ainsi, dans l'affaire *Segersted-Wiberg c. Suède*[10], la Cour a relevé en particulier, que, selon l'article 33 de la loi de 1998 sur les données de la police, des informations personnelles pouvaient être consignées dans le fichier de la Sûreté lorsque ces informations concernaient une personne soupçonnée d'une activité criminelle menaçant la sécurité nationale ou d'une infraction terroriste, ou faisant l'objet d'un contrôle de sécurité, ou lorsqu'il existait « d'autres raisons spéciales, eu égard au but de la tenue du fichier ». Si la Sûreté disposait d'une certaine latitude quant à l'appréciation de l'existence de « raisons spéciales », cette latitude n'était pas illimitée. Par exemple, en vertu de la Constitution suédoise, un citoyen ne pouvait faire l'objet d'une entrée dans un registre public exclusivement en raison de ses opinions politiques à moins qu'il y ait consenti. L'article 5 de la loi sur les données de la police interdisait également de manière générale la consignation de données sur la base des opinions politiques. Dans ces conditions, la Cour a estimé que l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités étaient définies avec suffisamment de clarté, compte tenu du but légitime poursuivi par la mesure en question, pour fournir à l'individu une protection adéquate contre l'arbitraire.

La question de la mémorisation des données collectées dans un registre secret et de sa durée est également importante. Elle est au cœur de l'affaire *Rotaru c. Roumanie*[11], dans laquelle la Cour a constaté une violation de la

[10] Arrêt Segersted-Wiberg c. Suède du 6 juin 2006.
[11] Arrêt Rotaru c. Roumanie du 4 mai 2000.

Convention en raison du manque de prévisibilité de la base légale invoquée par les autorités nationales. Il convient de noter que, dans cette affaire, la Cour a également été sensible au fait que la législation ne fixait pas de limite quant à l'ancienneté des informations conservées et à la durée de leur conservation. Il n'y avait pas non plus de disposition relative aux personnes pouvant consulter les dossiers, à la nature desdits dossiers, à la procédure à suivre pour les consulter. En se montrant plus exigeante pour ce qui concerne les données relatives au « passé lointain » d'un requérant, la Cour réaffirme que chacun a, en quelque sorte, un droit à l'oubli. Ceci était d'autant plus le cas en l'espèce que certaines des informations recueillies étaient fausses et de nature à porter atteinte à la réputation du requérant.

De manière générale, ce que la Cour cherche à assurer c'est un juste équilibre entre les intérêts qui se trouvent en concurrence. Dans une des premières affaires dont elle ait eu à connaître en la matière, l'affaire *Klass c. Allemagne*[12], elle a rappelé que les sociétés démocratiques se trouvaient menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État devait être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. Mais, consciente du risque « de saper, voire de détruire, la démocratie au motif de la défendre » que fait courir toute mesure de surveillance secrète par les mesures de sécurité, la Cour affirmait « que les États ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée ». Toutefois, dans l'affaire Klass, et malgré cette position de principe très ferme, la Cour conclut à la non-violation de l'article 8 au motif que la loi contestée par les requérants (portant restriction du secret de la correspondance, des envois postaux et des télécommunications) était considérée comme nécessaire, dans une société démocratique, à la sécurité nationale, la

[12] Arrêt Klass c. Allemagne du 6 septembre 1978.

défense de l'ordre et la prévention des infractions pénales (article 8 § 2). Elle a donc clairement pris en considération les intérêts en présence.

Dans l'affaire *Leander c. Suède*[13], le requérant se plaignait du fait que des données liées à ses activités syndicales passées aient été mémorisées et se soient trouvées à l'origine de sa perte d'emploi, car ledit emploi se trouvait situé à proximité d'une zone militaire et avait été classé comme dangereux pour la sécurité. La Cour a mis cette affaire à profit pour compléter et préciser sa jurisprudence. Tout d'abord en énonçant que la mémorisation dans un registre secret et la communication de données relatives à la vie privée d'un individu entraient bien dans le champ d'application de l'article 8 § 1 de la Convention européenne des droits de l'homme. Puis, la Cour fit application des restrictions prévues par l'article 8 § 2 et du fait que, dans une société démocratique, l'existence de services de renseignement et la conservation des informations peuvent s'avérer légitimes et prévaloir sur l'intérêt des citoyens, à condition de poursuivre des buts légitimes, à savoir la défense de l'ordre, la prévention des infractions pénales ou la protection de la sécurité nationale. Elle parvint donc à un constat de non-violation de l'article 8 au motif que les garanties dont s'entourait le système suédois de contrôle du personnel remplissaient les exigences de l'article 8. La Cour a estimé que le gouvernement suédois était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant.

Qui dit conservation des données dit fichage. Or, le fichage d'une certaine catégorie de la population peut parfois s'avérer nécessaire. Ainsi, dans les affaires *Bouchacourt c. France*, *Gardel c. France* et *M.B. c. France*[14], tout en réaffirmant le rôle fondamental de la protection des données personnelles soumises à un traitement automatique, surtout à des fins policières, la Cour a

[13] Arrêt Leander c/Suède du 26 mars 1987.
[14] Arrêts Bouchacourt c. France, Gardel c. France et M.B. c. France du 17 décembre 2009.

conclu que l'inscription des requérants au Fichier judiciaire national automatisé des auteurs d'infractions sexuelles, telle qu'elle leur avait été appliquée, n'était pas contraire à l'article 8. En effet, elle a considéré qu'elle ne saurait mettre en doute les objectifs de prévention du fichier en question, que les sévices sexuels constituent incontestablement un type odieux de méfaits et que les enfants et autres personnes vulnérables ont droit à la protection efficace de l'État dans ce domaine.

Toutefois, elle parvient parfois à la solution inverse. Ainsi, dans l'affaire *Khelili c. Suisse*[15] qui concernait la classification d'une ressortissante française comme « prostituée » dans la base de données informatique de la police de Genève pendant cinq ans. Dans son arrêt, la cour a noté que la mention « prostituée » comme profession avait été supprimée de la base de données informatisée de la police, mais que cette expression, jointe aux affaires pénales en relation avec les plaintes déposées contre la requérante, n'avait pas été corrigée. Cette expression figurait donc toujours dans les fichiers informatiques de la police. La Cour a donc conclu que la mémorisation, dans le dossier de police, d'une donnée à caractère personnel, prétendument erronée, avait violé le respect de la vie privée de M^me^ Khelili et elle a estimé que le maintien de la mention « prostituée » pendant des années n'était ni justifié, ni nécessaire dans une société démocratique.

Cette multiplication des fichiers est une constante des sociétés contemporaines. A chaque fois qu'un crime est commis par un récidiviste (notamment dans les affaires de mœurs), on entend les commentaires de ceux qui déplorent l'absence de fichiers permettant d'identifier les coupables potentiels. D'où l'apparition de fichiers de plus en plus complets contenant, par exemple, des données biométriques. Une des affaires importantes à cet égard est

[15] Arrêt Khelili c. Suisse du 18 octobre 2011.

l'affaire *S. et Marper c. Royaume-Uni*[16], qui concernait la conservation par les autorités des empreintes digitales, échantillons cellulaires et profils ADN des requérants après la conclusion, respectivement par un acquittement et par une décision de classement sans suite, des poursuites pénales menées contre eux.

Les empreintes digitales des requérants avaient été relevées dans le cadre de procédures pénales pour être ensuite enregistrées dans une base de données nationale, en vue de leur conservation permanente et de leur traitement régulier par des procédés automatisés à des fins d'identification criminelle.

La Cour a admis que la conservation des données relatives aux empreintes digitales et génétiques visait un but légitime, à savoir la détection et, par voie de conséquence, la prévention des infractions pénales. Elle a relevé que des empreintes digitales, des profils ADN et des échantillons cellulaires, constituaient toutes des données à caractère personnel au sens de la Convention du Conseil de l'Europe de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Selon la Cour, la législation interne doit ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention. La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières.

Quels sont les principes généraux dégagés par la Cour ?

L'intérêt des personnes concernées et de la collectivité dans son ensemble à voir protéger les données à caractère personnel, et notamment les données relatives aux empreintes digitales et génétiques, peut s'effacer devant l'intérêt légitime que constitue la prévention des infractions pénales. Cependant, compte

[16] Arrêt S. et Marper c. Royaume-Uni du 4 décembre 2008.

tenu du caractère intrinsèquement privé de ces informations, la Cour se doit de procéder à un examen rigoureux de toute mesure prise par un État pour autoriser leur conservation et leur utilisation par les autorités sans le consentement de la personne concernée.

Dans l'affaire S. et Marper, la Cour s'est donc penchée sur le point de savoir si la conservation des empreintes digitales et données ADN des requérants, qui avaient été soupçonnés d'avoir commis certaines infractions pénales, mais n'avaient pas été condamnés, était nécessaire dans une société démocratique. Elle a relevé que l'Angleterre, le pays de Galles et l'Irlande du Nord étaient les seuls ordres juridiques au sein de Conseil de l'Europe à autoriser la conservation illimitée des empreintes digitales et des échantillons et profils ADN de toute personne, quel que soit son âge, soupçonnée d'avoir commis une infraction emportant inscription dans les fichiers de la police.

Elle est parvenue à la conclusion que la protection offerte par l'article 8 serait affaiblie de manière inacceptable, si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part. Tout État qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière.

Dans cette affaire, la Cour a été frappée par le caractère général et indifférencié du pouvoir de conservation en vigueur en Angleterre et au pays de Galles. En particulier, les données en cause pouvaient être conservées quelles que soient la nature et la gravité des infractions dont la personne était à l'origine soupçonnée et indépendamment de son âge ; la conservation n'était pas limitée dans le temps ; et il n'existait que peu de possibilités pour un individu acquitté

d'obtenir l'effacement des données de la base nationale ou la destruction des échantillons.

La Cour a estimé particulièrement préoccupant le risque de stigmatisation, qui découlait du fait que les personnes dans la situation des requérants, qui n'avaient été reconnus coupables d'aucune infraction et étaient en droit de bénéficier de la présomption d'innocence, étaient traitées de la même manière que des condamnés. Certes, la conservation de données privées concernant les requérants n'équivalait pas à l'expression de soupçons. Néanmoins, l'impression qu'avaient les intéressés de ne pas être considérés comme innocents se trouvait renforcée par le fait que les données les concernant étaient conservées indéfiniment, tout comme celles relatives à des personnes condamnées, alors que celles concernant des individus n'ayant jamais été soupçonnés d'une infraction devaient être détruites.

En conclusion, la Cour a estimé que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur avait outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation en cause s'analysait en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne pouvait passer pour nécessaire dans une société démocratique. La Cour a conclu à l'unanimité qu'il y avait eu en l'espèce violation de l'article 8.

La divulgation des données

Une fois les données collectées et conservées, se pose une troisième question qui est celle de la divulgation de ces données. Elle est particulièrement sensible dans le domaine de la santé.

Une affaire importante à cet égard est l'affaire *Z c. Finlande*[17] à l'occasion de laquelle un tribunal avait condamné une personne, révélant par là même occasion la séropositivité de son épouse. La Cour a conclu à la violation de la Convention, en raison du rôle fondamental que joue la protection des données à caractère personnel dans le domaine de la santé. D'où l'importance de respecter le caractère confidentiel des informations qui y ont trait. Il y va de la confiance que les personnes accordent à leurs médecins et au système de santé en général. Dans le cas de l'affaire précitée, le caractère sensible de l'information divulguée rendait d'autant plus nécessaire le respect de la confidentialité, d'où le constat de violation auquel la cour est parvenue.

L'affaire *M.S. c. Suède*[18] a également permis à la Cour de rappeler que « la protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention. Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général. La législation interne doit donc ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention ». Toutefois, dans cette affaire, la Cour n'a pas constaté la violation de l'article 8. D'abord elle a noté que le dossier médical de M^{me} M.S. avait été communiqué par un organe public à un autre organe public, chargé d'apprécier si l'intéressée remplissait les conditions légales pour l'obtention d'une prestation qu'elle avait elle-même sollicitée. Elle a estimé que, pour décider s'il y avait lieu d'accueillir la demande

[17] Arrêt Z.c. Finlande du 25 février 1997.
[18] M.S. c. Suède du 27 août 1997.

d'indemnisation en cause, la Caisse avait un besoin légitime de vérifier les informations soumises par la requérante et de les confronter à celles que possédait le service de gynécologie. En l'absence d'informations objectives de la part d'une source indépendante, la Caisse aurait eu des difficultés à juger du bien-fondé de la demande. Par ailleurs, eu égard aux circonstances, la mesure litigieuse était soumise à des limitations importantes et assortie de garanties effectives et satisfaisantes contre les abus.

Dans l'affaire Peck précitée, qui concernait la vidéosurveillance, la Cour est parvenue à un constat de violation de l'article 8 en raison de la divulgation dans les médias d'une séquence enregistrée dans la rue par une caméra de télévision en circuit fermé de la mairie, laquelle montrait le requérant en train de se trancher les veines.

L'effet horizontal de la jurisprudence impose d'ailleurs aux États de prendre des mesures pour renforcer la confidentialité des données personnelles en matière médicale. Ainsi, dans les affaires *Biriuk et Armonas c. Lituanie*[19], la Cour a insisté sur le fait qu'il est indispensable que le droit interne garantisse la confidentialité des informations concernant les patients et empêche toute divulgation de données personnelles, eu égard tout particulièrement à l'impact négatif de telles divulgations sur la propension d'autres personnes à se soumettre volontairement à des tests de dépistage du HIV et aux traitements appropriés.

L'accès aux données

Cet exposé ne serait pas complet si la question du droit d'accès de toute personne aux données la concernant n'était pas abordée. Cette question se trouve au centre de l'affaire Gaskin[20]. Dans cette affaire, le requérant avait été placé suite au décès de sa mère, sous l'assistance de la commune de Liverpool. Aux

[19] Arrêts Biriuk et Armonas c. Lituanie du 25 novembre 2008.
[20] Arrêt Gaskin c. Royaume-Uni du 7 juillet 1989.

termes du Règlement de 1955 sur le placement des enfants, l'autorité locale se trouvait tenue de conserver certains dossiers confidentiels relatifs au requérant. Ce dernier, qui se plaignait d'avoir été maltraité, demanda la communication des notes et des dossiers établis par l'autorité locale pendant la période durant laquelle il fut pupille de l'assistance. Le gouvernement s'y opposait et déclarait, notamment, que le fonctionnement adéquat du service d'assistance à l'enfance dépendait des informations fournies par un certain nombre de personnes et qu'il était nécessaire de préserver l'anonymat de ces informateurs si on souhait qu'ils continuent de collaborer. La Cour a estimé qu'un système qui subordonnait l'accès aux dossiers à l'acceptation des informateurs, comme au Royaume-Uni, pouvait en principe être tenu pour compatible avec l'article 8 (art. 8), eu égard à la marge d'appréciation de l'État. Toutefois, quand un informateur n'est pas disponible ou refuse abusivement son accord, il doit sauvegarder les intérêts de quiconque cherche à consulter des pièces relatives à sa vie privée et familiale; il ne cadre avec le principe de proportionnalité que s'il charge un organe indépendant, au cas où un informateur ne répond pas ou ne donne pas son consentement, de prendre la décision finale sur l'accès. Or il n'en allait pas ainsi dans l'affaire Gaskin. D'où le constat de violation opéré par la Cour.

Toutefois, le droit d'accès aux données personnelles n'est pas absolu et une marge d'appréciation a pu être laissée à l'État, lorsque le fichier auquel l'accès était sollicité avait pour objet de protéger la sûreté de l'État ou la prévention des infractions. Ainsi, on peut citer l'arrêt *Segersted-Wiberg c. Suède*[21] dans lequel les requérants demandaient tous en vain à consulter l'intégralité des dossiers les concernant détenus par la Sûreté suédoise. Leurs demandes furent rejetées au motif que le fait de leur donner accès à leurs dossiers pouvait compromettre la prévention des infractions pénales ou la protection de la sécurité nationale. Se fondant sur le chapitre 5, article 1 § 2, de

[21] Arrêt Segerstedt-Wiberg c/ Suède du 6 juin 2006.

la loi de 1980 sur le secret, les autorités et les juridictions nationales estimèrent qu'il était « difficile de déterminer si les informations [pouvaient] être révélées sans compromettre le but des mesures prises ou prévues, ou nuire à des opérations futures ». La Cour a reconnu qu' « un refus d'accès intégral à un fichier de police secret au niveau national est nécessaire lorsque l'État peut légitimement craindre que la communication de telles informations risque de compromettre l'efficacité du système de surveillance secrète destiné à protéger la sécurité nationale et à lutter contre le terrorisme ».

Mesdames, Messieurs,

Que ce soit au niveau national ou au niveau européen, la protection des données personnelles aura été considérablement améliorée depuis le début des années soixante-dix. Des instances et des mécanismes de protection ont été créés et des conventions ont été adoptées.

Je considère que le rôle joué par des commissions telles que la vôtre est crucial. Mais la Cour européenne des droits de l'homme y contribue également par les développements de sa jurisprudence. J'espère que mon exposé vous l'aura démontré. Je vous remercie.