RFDA 2009 p. 741

L'affaire *Marper c/ Royaume-Uni* : un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne

Sylvie Peyrou-Pistouley, Maître de conférences à la Faculté de Bayonne, CDRE (EA 3004)

*
**

L'onde de choc des attentats du 11 septembre 2001 à New York n'en finit pas de se propager et les dégâts collatéraux ainsi produits se révèlent pour le moins inattendus. En effet, depuis 2001, la préoccupation première des démocraties occidentales est devenue celle de la lutte contre le terrorisme, et ce de façon parfois quasi-obsessionnelle. Celle-ci se nourrit de coopération policière, de constitution de fichiers de données personnelles toujours plus nombreux et toujours plus détaillés, afin de détecter les terroristes, ou autres délinquants, réels ou en puissance, tissant de la sorte un réseau d'informations permettant de sanctuariser la forteresse Europe. Néanmoins, ce réflexe légitime d'autodéfense pose un problème évident aux démocraties européennes au regard des impératifs de la protection des droits fondamentaux. La question de la protection des données à caractère personnel est au coeur de cette problématique, tant les progrès technologiques en font un instrument privilégié et toute la difficulté ici tient donc « aux contradictions fortes entre la volonté d'empêcher le terrorisme de frapper et la nécessité de protéger les droits de l'homme » (1).

C'est pourquoi l'arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire *S. et Marper c/ Royaume-Uni*, le 4 décembre 2008 (2) est, osons le mot, un « arrêt historique » (3). Les faits étaient les suivants : le premier requérant, S., né en 1989, fut arrêté le 19 janvier 2001 - il était donc âgé de 11 ans - et inculpé de tentative de vol avec violences. On releva ses empreintes digitales et on lui préleva des échantillons d'ADN ; il fut acquitté le 14 juin 2001. Le deuxième requérant, *Marper*, né en 1963, fut arrêté le 13 mars 2001 et inculpé de harcèlement à l'égard de sa compagne. On releva également ses empreintes digitales et on lui préleva des échantillons d'ADN. Après le retrait de la plainte par sa compagne, l'affaire fut classée sans suite le 14 juin 2001.

Les deux requérants demandèrent dès lors la destruction des empreintes digitales et échantillons d'ADN les concernant, d'abord aux autorités de police, puis par voie juridictionnelle, mais en vain (rejet de leur demande le 22 mars 2002 par le tribunal administratif, le 12 septembre 2002 par la cour d'appel, et enfin le 22 juillet 2004 par la Chambre des Lords). En effet, les données en question avaient été stockées sur la base d'une loi de 1984 sur la police et les preuves en matière pénale, qui autorise leur conservation pour une durée illimitée. Pour le législateur britannique, l'objectif de prévention ou détection des infractions pénales l'emporte en effet sur toute autre considération, y compris celle du droit au respect de la vie privée ; « il est dans l'intérêt public que la police dispose d'une base de données aussi grande que possible dans le cadre de la lutte contre la criminalité », notait le Lord Justice Waller devant la cour d'appel.

Les requérants se sont alors adressés à la Cour européenne des droits de l'homme, estimant que la conservation de leurs empreintes digitales et données ADN pour une durée illimitée, alors que l'un avait été acquitté, et l'autre avait vu son affaire classée sans suite, était constitutive d'une atteinte à leur droit au respect de leur vie privée, garanti par l'article 8 de la Convention européenne des droits de l'homme (CEDH). Celui-ci proclame dans son § 1 que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance », mais admet néanmoins dans son § 2 la possibilité d'une ingérence d'une autorité publique dans l'exercice de ce droit, mais « pour autant que cette ingérence est prévue par la loi et qu'elle 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 de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

La référence à l'article 8 de la Convention européenne des droits de l'homme (Conv. EDH) pose dès lors deux séries de questions. Il convient de savoir d'abord si la conservation d'empreintes digitales et de données ADN peut être analysée comme une atteinte au droit au respect de la vie privée, et de déterminer ensuite si cette atteinte est justifiée, c'est-à-dire si elle peut apparaître comme « nécessaire dans une société démocratique ». La Cour, ayant déjà développé une abondante jurisprudence sur la protection des données personnelles rattachée au domaine de l'article 8, répond par l'affirmative à la première question, et, s'agissant de la deuxième, prononce une condamnation vigoureuse - à l'unanimité, il faut le souligner - de la législation britannique, en tant qu'elle permet la conservation des données susmentionnées pour une durée illimitée ; elle y voit en effet une « atteinte disproportionnée au droit des requérants au respect de leur vie privée [qui] ne peut passer pour nécessaire dans une société démocratique » (4). Ce contrôle de proportionnalité, qui permet de mettre en balance l'intérêt des individus à la protection de leur vie privée et l'intérêt général lié à la prévention des infractions pénales, constitue l'axe principal du raisonnement suivi par la Cour ici. La condamnation exemplaire du Royaume-Uni en matière de protection des données personnelles sur la base de l'article 8 de la Conv. EDH soulève donc un certain nombre d'interrogations quant à ses répercussions.

L'arrêt de la Cour intervient en effet dans un contexte européen ultrasécuritaire, tout particulièrement au sein de l'Union européenne, marqué par une intensification de la coopération policière et judiciaire, pour l'édification d'un « espace de liberté, de sécurité et de justice », largement animé d'ailleurs par les autorités britanniques. Cette coopération policière et judiciaire en matière pénale prend forme par la mise en place de nombreux fichiers, afin de faciliter l'échange de données entre partenaires européens, le « principe de disponibilité » adopté à La Haye en 2004 (5) parachevant le système en instituant l'objectif, pour les services répressifs des États membres de l'Union européenne, « d'un accès plein et entier à toutes les données figurant dans toutes les bases de données nationales et européennes » (6). L'arrêt *Marper* de la Cour européenne des droits de l'homme ne manquera pas dès lors de produire ses effets dans ce domaine, d'autant que les fichiers mis en place semblent le plus souvent assortis de conditions de protection *a minima*, comme nous le verrons. La position de la Cour européenne des droits de l'homme apparaît ainsi pour le moins opportune, pour ne pas dire cruciale, dans ce contexte préoccupant pour la défense des libertés individuelles, où la Cour, en posant de nouvelles règles du jeu, s'invite nécessairement dans les débats du législateur européen. Le principe de proportionnalité, qui constitue donc l'outil majeur dont elle use dans son raisonnement, va par voie de conséquence devenir la clef de voûte de tout l'édifice de la protection des données en Europe. Cette certitude vaut plus particulièrement au sein de l'espace de liberté, sécurité et justice de l'Union européenne.

Le contrôle de la proportionnalité, instrument du contrôle juridictionnel en matière de protection des données

La conservation d'empreintes digitales et de données ADN (7) par les autorités policières britanniques, pour une durée illimitée et concernant deux requérants impliqués dans des poursuites pénales, malgré l'acquittement de l'un et le classement de l'affaire sans suite pour l'autre, posait un problème de principe évident. La Cour va conduire son raisonnement de manière très classique au regard de l'article 8 de la Conv. EDH en s'interrogeant en premier lieu sur l'existence d'une ingérence dans la vie privée des requérants par les mesures incriminées, puis en second lieu sur la justification d'une telle ingérence. Si l'ingérence dans la vie privée des requérants est avérée, la question du « juste

équilibre » entre les intérêts en présence, apprécié par la Cour dans le cadre du contrôle de proportionnalité entre la conservation des données (qui caractérise l'ingérence) et la finalité pour laquelle celles-ci sont recueillies (la nécessité de l'ingérence dans une société démocratique), constitue le point fort de l'argumentation de la Cour ici.

Une ingérence avérée dans la vie privée des requérants

La Cour, après avoir constaté dans un premier temps que la conservation d'empreintes digitales et de données ADN constitue en soi une ingérence au sens de l'art. 8 de la Convention, va vérifier dans un second temps l'existence d'une base légale sur laquelle cette ingérence puisse s'appuyer.

1) Après avoir rappelé que la notion de « vie privée » (8) doit être entendue de la manière la plus extensive possible (9), la Cour de Strasbourg rappelle le principe, clairement établi depuis l'arrêt *Leander (10)*, selon lequel « le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 » (§ 67). Pour constater cette ingérence en l'espèce, la Cour mène une analyse séparée concernant les deux catégories de données conservées par les autorités, distinguant les données ADN d'une part (profils ADN et échantillons cellulaires) et les empreintes digitales d'autre part.

Concernant les données ADN d'abord et plus particulièrement les échantillons cellulaires, la Cour avait déjà été confrontée à un tel cas de figure dans l'affaire *Van der Velden (11)*. Elle avait estimé que « la conservation systématique de pareils éléments (...) revêt un caractère suffisamment intrusif pour constituer une atteinte au droit au respect de la vie garanti par l'article 8 § 1 de la Convention, eu égard notamment à l'utilisation ultérieure qui pourrait être faite à l'avenir des échantillons cellulaires en question ». La même logique de raisonnement prévaut ici, mais de façon encore plus restrictive eu égard à « la nature » et à « la quantité des informations personnelles contenues » dans ces échantillons cellulaires (12). En effet, même la question de l'utilisation ultérieure qui pourrait en être faite (prise en considération dans l'affaire *Van der Velden*) importe peu (13), leur simple conservation « doit passer pour constituer en soi une atteinte au respect de la vie privée des individus concernés » (§ 73). Quant aux profils ADN (14), la Cour souligne en premier lieu qu'ils peuvent permettre de « découvrir les relations génétiques pouvant exister entre des individus » (§ 75), et surtout qu'ils offrent la possibilité de déterminer l'origine ethnique de la personne concernée, qui constitue une donnée sensible au titre de la Convention 108 du Conseil de l'Europe, ce qui justifie dès lors une protection accrue. L'atteinte au droit des requérants au respect de leur vie privée est par conséquent identifiée sans difficulté dans la simple conservation d'échantillons cellulaires et profils ADN.

La solution était-elle aussi évidente concernant les empreintes digitales ? Dans la mesure où elles ne contiennent pas autant d'informations sensibles, par leur quantité et leur nature, que les échantillons cellulaires et les profils ADN, la question de l'atteinte au droit au respect de la vie privée par leur simple conservation fait débat. Les précédents jurisprudentiels exploitables sont curieusement quasi inexistants. Cela dit, dans l'affaire *Kinnunen c/ Finlande (15)*, la Commission avait estimé que « les empreintes digitales n'impliquaient aucune appréciation subjective susceptible d'appeler une contestation et avait conclu que la conservation de pareils éléments n'était pas constitutive d'une atteinte à la vie privée » (16). Il faut noter en outre que les données en question avaient été effacées par la police ultérieurement à la demande du requérant.

L'arrêt *S. et Marper* procède sur ce point à un revirement de jurisprudence, la Cour s'affichant plus que jamais soucieuse d'assurer le respect de la vie privée des individus quand elle note que la conservation des empreintes digitales « sans le consentement de l'individu concerné, ne saurait passer pour une mesure neutre ou banale » (§ 84). Et même si leur conservation n'a évidemment pas la même portée que celle des données ADN, il n'en demeure pas moins que leur enregistrement « 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 » constitue « une atteinte au droit au respect de la vie privée » (§ 86). Cette conclusion est capitale, compte tenu du contexte européen que nous évoquerons plus loin (17).

2) La clause de restriction de l'article 8 § 2, qui énonce les conditions de justification d'une ingérence au droit garanti par le § 1, appelle classiquement une interprétation étroite (18). La Cour est amenée à examiner au préalable si l'ingérence peut s'appuyer sur une base légale. Pour ce faire, la Cour doit vérifier l'existence d'une base légale en droit interne, mais aussi son « accessibilité » et sa « prévisibilité », critères d'appréciation fixés depuis l'arrêt *Sunday Times* de 1979 (19).

En l'espèce, la Cour constate sans difficulté l'existence de la base légale en droit interne des mesures de conservation des empreintes digitales, des échantillons biologiques et des profils génétiques des requérants, en se référant à l'article 64 de la loi britannique de 1984 sur la police et les preuves en matière pénale. L'essentiel de son argumentation ici repose en fait - sans le dire - sur le caractère de « prévisibilité » de la loi eu égard aux conditions et modalités de mémorisation et d'utilisation de ces informations personnelles, sachant que la prévisibilité « se mesure à la précision et à la clarté de la loi » (20). La Cour estime sur ce point que « l'article 64 est beaucoup moins précis ». Déjà, dans l'arrêt *Rotaru c/ Roumanie (21)* - arrêt dans lequel la Cour, pour la première fois « affirme sans ambiguïté que l'article 8 de la Convention offre une protection vis-à-vis du traitement des données à caractère personnel » (22), la Cour avait jugé que « le système roumain de collecte et d'archivage d'informations [par le SRI - Service roumain de renseignements] » ne fournissait pas les meilleures garanties s'agissant des procédures de contrôle, qui doivent être normalement assurées par le pouvoir judiciaire, car « aucune procédure de contrôle n' [était] prévue par la loi » ; ce constat avait permis à la Cour de conclure que le droit interne n'indiquait pas « avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré » (§ 61). Une telle solution semble relever de la « procéduralisation » que semble pratiquer la Cour depuis l'arrêt *Klass (23)*, qui fait qu'elle apprécie « la restriction apportée aux droits fondamentaux (...) en fonction des garanties procédurales entourant l'adoption des mesures opérant cette restriction » (24). Par ailleurs, dans l'arrêt *Amann c/ Suisse (25)*, la Cour a souligné, d'une part, que l'établissement, par l'autorité publique, de la fiche incriminée ne satisfaisait pas à la condition de prévisibilité, car la norme n'était pas « suffisamment claire et détaillée pour assurer une protection appropriée contre les ingérences des autorités dans le droit du requérant au respect de sa vie privée » (§ 58 et § 76). Sa conservation, d'autre part, s'est avérée injustifiée, les autorités n'ayant pas détruit les renseignements mémorisés conformément au droit suisse, qui prévoit « la destruction des données qui ne s'avèrent plus nécessaires ou sont devenues inutiles »(§ 78) (26).

Dans l'affaire *Marper*, si la Cour insiste sur l'importance de « fixer des règles claires et détaillées » s'agissant du stockage, pour une durée illimitée il faut le rappeler, et de l'utilisation des données, elle ne se prononce pas justement sur le caractère clair et détaillé de la législation en l'espèce. Elle estime inutile de trancher la question de la qualité de la loi, considérant que le problème est étroitement lié « à la question plus large de la nécessité de l'ingérence dans une société démocratique » (§ 99), à laquelle elle renvoie. Cette « interférence » entre les deux problématiques (clarté de la loi/nécessité de l'ingérence dans une société démocratique) découle en réalité de la lettre même de l'article 64 de la loi britannique de 1984, qui dispose que les empreintes digitales et échantillons cellulaires « ne doivent pas être utilisés par quiconque, sauf à des fins en rapport avec la prévention ou la détection des infractions pénales, l'enquête sur une infraction ou la conduite de poursuites ». Sans doute est-il paru difficile à la Cour de se prononcer uniquement sur le critère de la « qualité » de la loi, et ce pour essentiellement deux raisons, semble-t-il. La première est que, contrairement à des affaires semblables, telles que *Rotaru* précitée (27) ou *Liberty et autres c/ Royaume-Uni (28)*, les dispositions de la loi concernent ici pour l'essentiel le principe même de la conservation pour une durée illimitée de certaines données

personnelles (ADN et empreintes digitales) collectées à l'occasion de procédures judiciaires pénales. Par conséquent, sans même envisager la question des détails de la conservation et des modalités d'utilisation de ces données, il est apparu plus important au juge d'examiner directement la question - en quelque sorte préalable, même si dans le raisonnement elle est opérée postérieurement - de la nécessité « dans une société démocratique » de la conservation de telles données pour une durée illimitée. La deuxième raison tient à l'importance de l'affaire au fond. La législation du Royaume-Uni sur cette question de la conservation d'empreintes digitales et de données ADN pour une durée illimitée apparaît comme particulièrement attentatoire aux droits fondamentaux. Il est permis d'imaginer que la Cour a préféré statuer au fond sur la question cruciale de la nécessité de la mesure dans une société démocratique, afin de donner une plus grande portée à la solution adoptée, compte tenu de l'importance de l'enjeu.

Une ingérence disproportionnée

La Cour doit ici résoudre la question de savoir si la conservation litigieuse des données des requérants, qui constitue une ingérence dans leur vie privée, est « nécessaire dans une société démocratique », selon les termes de l'article 8 § 2 de la Convention. La notion classique de marge d'appréciation permet à la Cour, dans un premier temps, de poser le cadre à l'intérieur duquel elle pourra apprécier dans un second temps la proportionnalité de l'ingérence contestée, c'est-à-dire le juste équilibre entre les intérêts publics et privés.

1) Les développements que la Cour consacre à l'examen de la condition de la nécessité de la mesure dans une société démocratique, constituent le coeur de son raisonnement. Ceci ne surprend pas, car « la notion de "société démocratique" est bien la valeur centrale de "l'ordre public européen" autour duquel s'ordonne aujourd'hui le droit européen des droits de l'homme » (29).

L'articulation entre la nécessaire autonomie laissée à chaque État pour déterminer une ingérence dans le droit garanti, comme le permet le § 2 de l'article 8, et le non moins indispensable contrôle du juge européen se situe dans la notion de marge d'appréciation. La Cour rappelle son principe et le développe amplement dans le cas d'espèce. Et la présentation des principes par la Cour dans l'affaire étudiée montre dès l'abord qu'il s'agit de mettre en balance des intérêts contradictoires : l'intérêt de la protection des données à caractère personnel, qui « joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacrée par l'article 8 de la Convention » (§ 103), et « l'intérêt légitime que constitue la prévention des infractions pénales » (30). Cela dit, en l'espèce, la Cour restreint le champ de la question examinée. Celle-ci n'est pas en réalité de savoir, il faut le souligner, si la conservation des empreintes digitales, échantillons cellulaires et profils ADN en général est justifiée au regard de la Convention, mais plus exactement de savoir si la conservation de telles données des requérants « qui avaient été soupçonnés d'avoir commis certaines infractions pénales mais n'avaient pas été condamnés se justifiait sous l'angle de l'article 8 § 2 de la Convention » (§ 106). Pour répondre à cette question, la Cour va rechercher si l'ingérence est proportionnée au but légitime poursuivi, le principe de proportionnalité, « qui traduit une exigence d'adéquation entre un objectif légitime et les moyens utilisés pour l'atteindre, se [situant] donc au coeur du contrôle de la marge nationale d'appréciation » (31). Deux paramètres sont déterminants ici dans la démarche du juge : la perspective comparatiste, qui lui permet de déplacer le curseur du contrôle de la marge d'appréciation, et la vérification du « juste équilibre » entre l'intérêt général et les intérêts de l'individu (32).

Déjà, dans la première partie de son arrêt (« en fait »), la Cour avait pris soin de recenser de façon détaillée les textes pertinents en la matière, issus non seulement du droit et de la pratique des États membres, mais également produits au niveau européen, tant par le Conseil de l'Europe que par l'Union européenne. C'est dire l'importance des enjeux et la complexité de la situation engendrée (nous y reviendrons).

L'étude des législations des États est particulièrement importante, car de cela va dépendre l'étendue de la marge d'appréciation laissée à l'État défendeur. Si la Cour n'arrive pas à identifier des « conceptions communes aux États parties sur certains buts légitimes d'ingérence » (33), la marge laissée à l'État sera plus ample. Par exemple, dans son arrêt *Rasmussen (34)*, la Cour a noté à quel point « la présence ou absence d'un dénominateur commun aux systèmes juridiques des États » est pertinente en la matière. La Cour se livre ici de façon très appliquée à cette interprétation dite « consensuelle », ce qui la conduit à constater que « l'Angleterre, le Pays de Galles et l'Irlande du Nord sont les seuls ordres juridiques au sein du 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 important inscription dans les fichiers de la police » (§ 110). Dans la plupart des États contractants en effet, non seulement la conservation de telles données est limitée aux individus soupçonnés d'avoir commis des infractions présentant un certain seuil de gravité, mais encore les données ADN doivent être détruites ou effacées soit immédiatement soit dans un certain délai après un acquittement ou un non-lieu.

Si l'interprétation consensuelle peut certes paraître souvent comme « le masque du pouvoir discrétionnaire du juge européen » (35), force est de constater ici que la spécificité législative britannique n'apparaît pas comme un « particularisme local » dont l'application de la Convention pourrait s'accommoder - compte tenu du « rôle de pionnier dans l'évolution de nouvelles technologies » que revendique le Royaume-Uni - mais plutôt comme une mesure disproportionnée eu égard aux intérêts en présence, intérêts dont il convient de vérifier le « juste équilibre ». Le coeur du problème se situe ici dans le fait que les empreintes digitales et échantillons cellulaires des requérants ont été prélevés dans le cadre de procédures pénales engagées à leur encontre, puis ont été stockées pour une durée illimitée, alors même que le premier requérant a été acquitté et que le second a vu son affaire classée sans suite. La Cour prend en considération l'argumentation du gouvernement britannique selon laquelle l'élargissement de la base de données contribue à la détection et à la prévention des infractions pénales ; il n'en demeure pas moins indispensable de « déterminer si pareille conservation est proportionnée et reflète un juste équilibre entre les intérêts publics et privés qui se trouvent en concurrence » (§ 118).

2) Dans l'affaire *Leander (36)*, où le requérant se plaignait de n'avoir pu occuper un poste permanent au musée naval de Karlskrona (jouxtant une base militaire interdite d'accès), à cause d'informations secrètes qui l'auraient présenté comme dangereux pour la sécurité nationale, la Cour avait pu estimer que le gouvernement défendeur jouissait en l'espèce d'une large marge d'appréciation (37). Il était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant (§ 67 de l'arrêt).

Dans l'affaire *Z. c/ Finlande* en revanche (38), où le juge soulignait que l'ampleur de la marge d'appréciation « est fonction de facteurs tels que la nature et l'importance des intérêts en jeu et la gravité de l'ingérence » (§ 99), la Cour avait jugé que la production de documents médicaux lors d'un procès, passé le délai légal de confidentialité de dix ans, constituait « une ingérence disproportionnée dans le droit de la requérante au respect de sa vie privée et familiale, au mépris de l'article 8 » (§ 112 de l'arrêt), de même que la publication de son identité et de son état de santé dans l'arrêt, rendu public, de la cour d'appel d'Helsinki, « a porté atteinte... au droit au respect de la vie privée et familiale garanti par l'article 8 » (§ 113). Dans un arrêt *Segerstedt-Wiberg et autres c/ Suède (39)*, la Cour avait également pensé que l'État était « en droit de considérer que les intérêts de la sécurité nationale et de la lutte contre le terrorisme l'emportent sur les intérêts des requérants à être informés de l'intégralité des informations les concernant conservées dans les fichiers de la sûreté ». Peut-être cette solution était-elle transposable - *mutatis mutandis* - dans l'affaire *Marper*, mais dans l'affaire *Segerstedt*, la Cour avait noté que l'État défendeur disposait d'une « ample marge d'appréciation », ce qui n'est pas le cas en l'espèce.

Ici, deux éléments vont être déterminants : d'abord le caractère général et indifférencié du pouvoir de conservation des données en cause, quelles que soient la nature et la gravité des infractions dont la personne est soupçonnée et quel que soit son âge, et ensuite le fait que les données en question soient conservées indéfiniment, quelles que soient la nature et la gravité de l'infraction. Ce qui apparaît particulièrement choquant en l'espèce est que les données concernant les requérants - non condamnés - sont conservées indéfiniment comme celles de personnes condamnées (40). Ceci paraît difficilement conciliable avec la présomption d'innocence, les requérants, non condamnés, étant traités sur ce point de la même manière que les condamnés. « Exprimer des soupçons sur l'innocence d'un accusé une fois que celui-ci a été acquitté » (§ 122) « est incompatible avec la présomption d'innocence » (41). La conservation des données en l'occurrence ne place-t-elle pas les requérants - tout un chacun demain - dans la situation de délinquant potentiel ? Cette idée était corroborée par l'argumentation, maladroite, du gouvernement soulignant que les requérants n'étaient pas soupçonnés d'une infraction, mais que « son seul souci [était] d'augmenter la taille et donc l'usage de la base de données en vue de l'identification de criminels dans l'avenir » (*sic*).

La Cour conclut énergiquement son analyse en estimant 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 (...) ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique » (§ 125). Il y a bien eu violation de l'article 8 de la Convention, le contrôle de proportionnalité opéré par la Cour entre la conservation des données et le but pour lequel elles ont été recueillies lui permet de parvenir à ce jugement. La Cour souligne d'ailleurs ne pouvoir ignorer « le fait que, en dépit des avantages susceptibles de découler d'un élargissement maximal de la base de données ADN, d'autres États contractants ont décidé de fixer des limites à la conservation et à l'utilisation de telles données afin de parvenir à un équilibre adéquat avec l'intérêt concurrent (42) que constitue la préservation de la vie privée » (43).

Ce lien établi par le juge entre la conservation des données (et ses modalités) et la finalité pour laquelle elles sont collectées est essentiel, cette dernière conditionnant la régularité de la première. Il est le constat du « fort consensus » (44) qui existe au sein des États quant à cette « mise en balance attentive » (45) des intérêts contradictoires en présence. D'où la réduction de la marge d'appréciation dont disposait le Royaume-Uni en l'espèce.

Des zones d'ombre subsistent néanmoins.

Il n'est pas neutre de relever au passage que, sur la question du but légitime de la mesure de conservation des données relatives aux empreintes digitales et génétiques (qui constitue l'ingérence), la Cour s'en remet à l'argument du défendeur. Le Royaume-Uni met l'accent sur l'objectif « plus large » que la simple « prévention des infractions pénales », à savoir « contribuer à l'identification de futurs délinquants », ouvrant un véritable débat de principe. Peut-être la Cour aurait-elle pu se poser d'abord la question de savoir si la conservation des données de personnes impliquées dans des procédures judiciaires pénales conclues par un acquittement dans un cas et un abandon des poursuites dans l'autre, concourt à « l'identification de futurs délinquants » et si cette dérive conduit au point où tout citoyen est présumé délinquant en puissance (46).

Ensuite, quant au but général de la législation, que la Cour se doit d'apprécier ici de façon abstraite, on peut s'interroger sur le fait que la Cour n'a pas posé la question de savoir si « l'intérêt public [qui est celui] de détecter et poursuivre les infractions graves » (47), voire de « contribuer à l'identification de futurs délinquants » (§ 100), est susceptible effectivement de justifier le stockage systématique et pour une durée illimitée de données personnelles contenant des empreintes digitales et échantillons cellulaires, « suffisamment intrusi(f) pour entraîner une atteinte au droit au respect de la vie privée » (§ 70) ? La curieuse timidité de la Cour sur ce point semble néanmoins s'inscrire dans une certaine continuité jurisprudentielle, car, d'une manière générale, « la Cour européenne est attentive à ne pas contester les objectifs invoqués par le gouvernement défendeur pour justifier une restriction à un droit garanti, se limitant à émettre 'des doutes' en la matière » (48). Elle n'en a émis aucun ici, et on peut déplorer qu'elle ait avalisé comme « but légitime », sans autre forme de procès, l'argument avancé par le Royaume-Uni. Entre l'objectif de protection des droits individuels et celui de sécurité publique, il semble que ce soit le choc du pot de terre contre le pot de fer...

Soulignons, pour terminer, que si le contrôle exercé par la Cour est un contrôle subsidiaire, il semble que ce soit ici la fonction substantielle de la subsidiarité qui s'impose, en tant qu'elle opère une répartition des compétences entre les États et les organes de la Convention (49). En effet, la Cour, qui met en oeuvre son critère d'évaluation relatif à la marge d'appréciation, semble le faire dans le sens où c'est elle qui se reconnaît le mieux à même de contrôler la nécessité de l'ingérence (ce qui rappelle l'idée de subsidiarité au sens communautaire du terme). Elle le fait en exerçant un contrôle plein et entier, qui semble confiner à l'opportunité, et pas seulement à la régularité de la mesure prise par l'État. On ne peut qu'approuver cette démarche, « cette notion [fournissant] au juge de Strasbourg un standard d'interprétation fort utile qui lui permet de mener une véritable politique jurisprudentielle » (50).

En ces temps marqués par des préoccupations sécuritaires grandissantes face à la criminalité ou au terrorisme, au détriment des droits fondamentaux, où la mise en balance des intérêts semble perdue d'avance pour les droits individuels, la Cour de Strasbourg, par l'arrêt *Marper*, se place délibérément au centre de tous les dispositifs en matière de protection des données. L'instrument de la proportionnalité, clef de voûte de son raisonnement comme nous venons de le voir, est appelé à devenir le pivot de la protection des données en Europe, et plus particulièrement au sein de l'espace de liberté, sécurité et justice de l'Union européenne.

Le respect de la proportionnalité, condition préalable de la législation de l'espace de liberté, sécurité, justice

Au regard des insuffisances, tant des droits nationaux que du droit de l'Union en matière de protection des données à caractère personnel, la Cour va être amenée dans l'avenir à jouer un rôle déterminant, bien au-delà de la protection subsidiaire qu'elle assure normalement. Elle va dicter désormais la règle du jeu à suivre par les différents protagonistes, nationaux et européens, en posant la limite à ne pas franchir quant à l'utilisation des fichiers en matière pénale ou d'entraide répressive. L'insuffisance des dispositifs actuels de protection conduit le juge de Strasbourg à cette attitude avec le concours grandissant de la Cour de justice de l'Union.

L'insuffisance des dispositifs de protection des données au niveau de l'Union

La portée de l'arrêt *Marper* dépasse de loin l'intérêt des parties en cause. Dans un contexte européen de stockage - généralisé par les États - d'un nombre de plus en plus important de données personnelles à des fins répressives, la question se pose inévitablement de leur protection, s'agissant de leur conservation comme de leur partage. Le développement accéléré d'un flux considérable d'échanges de données au niveau de l'Union nourrit les motifs d'inquiétude.

1) L'existence de la collecte de données personnelles à des fins répressives au niveau des États n'est pas un fait nouveau, c'est l'ampleur que prennent ces fichiers qui apparaît aujourd'hui comme préoccupante (51). Dans l'arrêt *Marper*, la Cour en est consciente et focalise son étude sur les fichiers d'empreintes digitales et d'échantillons cellulaires

collectés dans le cadre de procédures pénales. Elle souligne à cet égard que « la majorité des États membres du Conseil de l'Europe autorisent le prélèvement obligatoire » de telles données (52) et ajoute que « le nombre de pays dans ce cas est en constante augmentation ». Néanmoins, la Cour est amenée à constater que dans la plupart de ces pays, le prélèvement de données ADN, plus spécifiquement, n'est opéré que « dans des circonstances particulières » ou pour les « infractions les plus graves » (53). Dès lors, le Royaume-Uni apparaît comme « le seul État membre à autoriser expressément la conservation systématique et pour une durée illimitée des profils ADN et échantillons cellulaires des personnes ayant bénéficié d'un acquittement ou de l'abandon des poursuites » (54). Il existe, nécessairement, dans tous les États membres des autorités et des mécanismes de contrôle concernant le prélèvement ou la conservation des données personnelles, définis par la législation nationale. Il semblerait sur ce point que, dans l'ensemble, les différences soient assez peu sensibles (55).

Cela dit, toutes les données collectées au niveau national ne constituent que le premier étage d'une construction plus complexe où le deuxième étage, européen, surajoute ses propres fichiers, afin d'assurer une coopération policière et judiciaire à grande échelle, ce pour répondre à des préoccupations sécuritaires de lutte contre la criminalité ou le terrorisme. On peut citer le SIS (système d'information Schengen), le SID (système d'information des douanes), EURODAC (concernant les demandeurs d'asile et les immigrants clandestins), le VIS (système d'information sur les visas), EUROPOL (Office européen de police), EUROJUST (pour la coopération judiciaire), le dispositif issu du Traité de Prüm désormais intégré dans le droit de l'Union (56), le tout sans parler des nombreuses propositions de la Commission actuellement pendantes et des accords passés avec des États tiers, comme les États-Unis. La liste parle d'elle-même pour évaluer l'importance du fichage au niveau européen. Mais la question principale qui se pose ici est bien celle du contrôle institué afin d'assurer la protection des données collectées : les motifs d'inquiétude s'avèrent ici nombreux.

2) La problématique des dispositifs mis en place en matière de protection des données à caractère personnel dans l'Union européenne concerne pour l'essentiel le troisième pilier de l'Union européenne (UE), tous les mécanismes d'entraide répressive s'appuyant sur la constitution de fichiers de données personnelles. Soulignons ici la grande complexité du système de fichage, puisqu'une part de traitement des données purement nationale et une part commune coexistent.

Pour la part nationale, les conditions de protection mises en oeuvre relèvent des différentes législations nationales. La place que prend la législation nationale est bien sûr proportionnelle à l'ampleur de cette part purement nationale de traitement des données : elle est importante dans le SIS par exemple (57), elle est plus faible dans EUROPOL (58) ou EURODAC (59). Le risque d'aboutir à des niveaux de protection très différents d'un pays à l'autre est évident mais il semblerait à l'analyse que cela ne soit pas le cas (60). La définition d'un socle commun en la matière était cependant indispensable dès lors que la circulation des données entre États membres en matière répressive s'intensifie. La question a été posée d'ailleurs lors des longues négociations relatives à l'adoption de la décision-cadre relative à la protection des données dans le troisième pilier (61), qui finalement écarte de son champ d'application les traitements purement internes. Cette façon de procéder a été vivement critiquée par le Contrôleur européen de la protection des données, dans ses trois avis relatifs à la proposition de décision-cadre (62). Il note en particulier dans le troisième que « l'applicabilité de la décision-cadre au traitement national des données est une condition essentielle afin, non seulement d'assurer un niveau de protection suffisant des données à caractère personnel, mais aussi de permettre une collaboration efficace entre les services répressifs ». De son point de vue, exact, « la possibilité d'avoir différents niveaux de protection des données des différents États membres dans le cadre du troisième pilier (...) serait incompatible avec la création d'un espace de liberté, de sécurité et de justice au sein duquel les citoyens se déplacent librement et avec un rapprochement approprié des législations conformément à l'article 34 § 2 point b) du traité UE » (63).

Les règles définies dans le cadre de l'UE ne sont pas inutiles. Il existe d'abord un certain nombre de règles spécifiques, au champ d'application limité au système d'échange de données qui les a vu naître, tous instaurés dans le cadre du titre VI du Traité UE relatif à la coopération policière et judiciaire en matière pénale - à ceci près que certains systèmes, comme le SID par exemple, relèvent à la fois du droit communautaire, c'est-à-dire du premier pilier, et de la coopération policière du troisième pilier. En matière de conservation par exemple, au coeur de la problématique de l'arrêt *Marper*, tous ces textes (64) ont pour point commun de prévoir la conservation des données « le temps nécessaire pour lui permettre (65) de remplir ses fonctions », ou autre formule analogue, plutôt vague, ouvrant la porte à une durée discrétionnaire de conservation par les autorités concernées. À la suite de l'arrêt *Marper*, la question risque de se poser de la régularité de ces dispositions au regard de la Conv. EDH. Tous les textes assurent par ailleurs un niveau de protection des données « au moins égal à celui résultant des principes de la Convention de Strasbourg de 1981 » et à prévoir la désignation d'une autorité de contrôle dans chaque État membre. Il est difficile de faire moins.

Dans le domaine purement communautaire, il existe un certain nombre de textes sur la protection des données. Le premier d'entre eux est la directive 95/46/CE 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 (66). Le problème majeur est qu'elle ne s'applique pas, par définition, aux activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du Traité UE, pas davantage qu'aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal (67). Par conséquent, l'ensemble des fichiers dont il est question ici ne peut bénéficier de sa protection. Même réserve concernant le règlement 45/2001 du Parlement européen et du Conseil du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (68), qui s'applique au traitement des données par toutes les institutions et organes communautaires, dans la mesure où ce traitement est mis en oeuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire (69). Le champ d'application de ces textes pose donc problème, malgré leur caractère tout à fait satisfaisant.

C'est la raison pour laquelle la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (70), a vocation à en constituer l'équivalent, pour le troisième pilier (71). Cette décision-cadre souffre cependant d'un grand nombre d'insuffisances. D'abord, comme l'indique le point 39 de l'exposé des motifs, l'ensemble des dispositions spécifiques relatives à la protection des données à caractère personnel résultant d'actes adoptés sur la base du titre VI du Traité UE, tels que EUROPOL, EUROJUST, le SIS, le SID et le dispositif du traité de Prüm intégré dans le traité par la décision 2008/615/JAI du Conseil du 23 juin 2008, ne devrait pas être affecté par la décision-cadre. Par conséquent, les dispositions spécifiques prévues par ces textes continueront à s'appliquer, avec toutes leurs limites. Il résulte, ensuite, du point 40 du même exposé des motifs que, dans la mesure où les dispositions relatives à la protection des données figurant dans des actes adoptés sur la base du titre VI du Traité UE, renvoient à la Convention 108 du Conseil de l'Europe et/ou contiennent des dispositions plus restrictives que celles de la décision-cadre, cette dernière n'a pas vocation à s'y substituer. Si cela peut être rassurant pour la deuxième hypothèse, ce choix reste très minimal dans la première. Il résulte encore de l'article 1 de la décision-cadre qui délimite son champ d'application, qu'elle ne concerne pas davantage tout ce qui est relatif au traitement national des données (72). Il faut ajouter au surplus que la décision-cadre ne s'applique pas non plus dès lors que sont en jeu « des intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale » (73).

Sur la question plus spécifique de la conservation des données, l'article 5 de la décision-cadre précise que « des délais

appropriés sont prévus pour effacer les données à caractère personnel ou vérifier régulièrement s'il est nécessaire de conserver les données ». Cette formulation laisse place à une grande marge d'appréciation. À qui, sous-entendu à quel juge, reviendra-t-il de la contrôler ?

Au total, quant au niveau de protection assuré par la décision-cadre - sans aller plus avant dans son analyse, qui dépasserait l'objet de cette étude - il n'est besoin que de se reporter à l'avis du contrôleur européen de la protection des données (CEPD) sur la question (74), qui constate que « le faible niveau de protection offert par la proposition ne saurait répondre aux besoins de la création d'un espace de liberté, de sécurité et de justice à l'intérieur duquel les autorités policières et judiciaires pourraient échanger des informations en matière répressive sans tenir compte des frontières nationales » (75).

Le principe de disponibilité doit être évoqué également comme particulièrement préoccupant du point de vue de la protection des droits fondamentaux. Ce principe, issu du « Programme de La Haye » (76), peut être défini comme la possibilité pour les services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions, de les obtenir d'un autre État membre qui les détient, en mettant ces informations à sa disposition (77). Cela va permettre l'instauration d'une coopération sans précédent entre États membres en matière d'échange de données à caractère personnel pour les domaines couverts par le troisième pilier, sachant que l'État membre sollicité est tenu de communiquer les informations requises sauf refus dûment motivé. Cette « mutualisation, à l'échelle communautaire, des informations des données des traitements nationaux » (78) pose de façon inédite la question du contrôle instauré en la matière. Ce principe de disponibilité en effet fait disparaître le lien qui est habituellement établi entre les données recueillies, et la finalité pour laquelle elles sont ainsi collectées. Le Contrôleur européen de la protection des données a manifesté son inquiétude à cet égard (79) ; il a d'abord souligné l'importance « de veiller à ce que la proposition ne favorise pas une interconnexion sans restriction des bases de données et, par conséquent, la création d'un réseau de bases de données qu'il sera difficile de contrôler » (80), et note surtout en remarque finale qu'il « convient de veiller tout particulièrement à garantir les principes de limitation de la finalité et de traitement ultérieur (...) » (81).

Le même Contrôleur européen de la protection des données a également exprimé sa préoccupation s'agissant du projet de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (*Passenger Name Record* - PNR) à des fins répressives (82). Ce texte apparaît comme étroitement lié à l'accord intervenu entre les États-Unis et l'UE le 23 juillet 2007 (83), et vise à harmoniser les dispositions des États membres en ce qui concerne l'obligation qu'ont les transporteurs aériens assurant des vols au départ ou à destination d'un ou plusieurs États membres, de transmettre aux autorités compétentes les données PNR afin de prévenir et de combattre les infractions terroristes et la criminalité organisée. Le CEPD s'inquiète de « cette étape supplémentaire vers une collecte systématique des données concernant des personnes qui, en principe, ne sont soupçonnées d'aucune infraction (84) » et constate qu'on « peut observer cette évolution aussi bien au niveau international qu'au niveau européen » (85). Rappelant à cet égard « l'existence d'autres systèmes à grande échelle visant à contrôler les déplacements de personnes à l'intérieur ou aux frontières de l'UE », comme le système d'information sur les visas (VIS) ou le système d'information Schengen (SIS), puis les bases de données de la police nationale contenant des données biométriques rendues accessibles grâce au système du Traité de Prüm (aujourd'hui intégré dans l'UE), le CEPD constate que « tous ces instruments permettent un contrôle global des déplacements de personnes, même si les buts recherchés diffèrent » puis note que « accumuler les bases de données sans disposer d'une vision globale des résultats (...) pourrait ouvrir la voie à une évolution vers une société de surveillance totale », et conclut enfin que « la lutte contre le terrorisme peut certainement constituer un motif légitime pour appliquer des exceptions aux droits fondamentaux à la vie privée et à la protection des données. Toutefois, pour être valable, la nécessité de l'ingérence doit s'appuyer sur des éléments clairs et indéniables, et la *proportionnalité du traitement* (86) doit être démontrée. Cette exigence s'impose d'autant plus dans le cas d'une atteinte considérable à la vie privée des personnes concernées, comme celle que prévoit la proposition » (87).

Cette condition de proportionnalité, posée comme condition sine qua non par le CEPD à l'entrée en vigueur de la proposition, est au coeur de l'arrêt *Marper*. L'intervention de la Cour européenne des droits de l'homme lui permet donc de se positionner au centre du système européen de protection des données.

L'apport de la Cour européenne au contrôle de la protection des données

En plaçant le principe de proportionnalité au coeur de son arrêt *Marper*, la Cour européenne des droits de l'homme s'impose comme l'ordonnateur de l'espace de liberté, sécurité, justice. Ce principe répond en effet à l'essentiel des inquiétudes qui se font jour au sein de l'Union et, en l'état du système contentieux de l'Union, c'est sans doute la Cour de Strasbourg elle-même qui se révèlera la mieux à même de le garantir.

1) La proportionnalité mise en avant par la Cour européenne apparaît comme la réponse la plus adaptée aux diverses inquiétudes formulées.

S'agissant, d'abord, du principe de disponibilité, il est bon de rappeler que l'une des clés d'analyse de la Cour dans son arrêt *Marper* consiste à vérifier si « la conservation des données [est] proportionnée au but pour lequel elles ont été recueillies et [si elle est] limitée dans le temps » (88). En l'espèce, la Cour condamne justement le Royaume-Uni pour la conservation illimitée de données à caractère personnel dans l'éventualité d'un hypothétique usage ultérieur de détection d'infractions pénales, ce qui rompt nécessairement « l'équilibre adéquat avec l'intérêt concurrent que constitue la préservation de la vie privée » (89). La mise en oeuvre du principe de disponibilité, dans la mesure où il rompt le lien entre les données recueillies et la finalité pour laquelle elles sont collectées, ne risque-t-elle pas dès lors de tomber sous les foudres du juge de Strasbourg ?

La question mérite d'autant plus d'être posée que la proposition de décision-cadre relative au principe de disponibilité prévoit dans son cinquième considérant que la décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (90) « s'applique aux traitements de données à caractère personnel réalisés par les États membres en vertu de la présente décision-cadre ». Or, justement, la décision-cadre « protection des données dans le troisième pilier » a suscité de vives critiques de la part du CEPD sur ce point (91). Le Contrôleur européen y rappelle au préalable que « le principe de limitation de la finalité est l'un des principes de base de la protection des données » et que « la jurisprudence de la Cour européenne des droits de l'homme a clairement établi que de telles exceptions devaient être *proportionnées* (92), précises et prévisibles, conformément à l'article 8 § 2 de la Convention européenne des droits de l'homme » (93). Il note ensuite que l'article 3 de la décision-cadre « est bien trop large et ne couvre pas une limitation appropriée de la finalité en vue de l'enregistrement », puis que « la référence générale aux finalités du titre VI du traité UE ne saurait être considérée comme des finalités spécifiques et légitimes. Les finalités de la coopération policière et judiciaire ne sont pas légitimes par nature » (94).

Cette opinion doit être rapprochée de l'arrêt *Marper*. La Cour de Strasbourg condamne la conservation illimitée de données à caractère personnel dans l'éventualité d'un hypothétique usage ultérieur de détection d'infractions pénales, qui entraîne la rupture de ce lien de finalité entre la collecte des données et l'utilisation qui en est faite. Cette rupture a pour conséquence de porter atteinte à « l'équilibre adéquat » entre intérêt public et intérêt privé : il n'y a donc plus

proportionnalité entre l'atteinte au droit protégé (droit au respect de la vie privée) et la nécessité de la mesure dans une société démocratique, comme le prescrit l'article 8 § 2 de la CEDH. Il apparaît donc au vu de ce jugement que non seulement la mise en oeuvre de la décision-cadre « protection des données dans le troisième pilier » risque de poser problème, mais que celle du principe de disponibilité est dans le même cas, ce principe étant appelé à devenir la pierre de touche de l'espace de liberté, sécurité, justice en organisant une « libre circulation » des informations nécessaires à la lutte contre la criminalité entre services répressifs au sein de l'Union européenne.

Ensuite, plus spécialement, il n'est pas certain que toutes les dispositions relatives à la protection des données contenues dans les textes spécifiques cités plus haut, tels que EUROPOL, EUROJUST, le SID etc., répondent à l'exigence de proportionnalité posée par la Cour. Concernant la question des délais de conservation en particulier, cela signifie qu'il faudra contrôler au cas par cas s'ils sont proportionnés au but à atteindre. Le doute est permis, compte tenu de l'imprécision des formules employées en la matière, qui laissent place à une marge discrétionnaire considérable pour les autorités concernées (95).

Enfin, la question de la proportionnalité dans la proposition de décision-cadre PNR évoquée nécessite de prendre en compte un certain nombre d'éléments. Le CEPD a d'ailleurs lui-même recensé les points faibles du texte (96). Il insiste sur le fait que « le respect du principe de proportionnalité suppose non seulement que la mesure proposée soit efficace, mais aussi que l'objectif poursuivi par la proposition ne puisse être atteint au moyen d'instruments portant moins atteinte à la vie privée ». Dans le même ordre d'esprit, il déplore que « l'efficacité des mesures n'a pas été démontrée » et conclut qu'il « convient d'examiner soigneusement l'existence de solutions alternatives avant de mettre en oeuvre des mesures supplémentaires et/ou nouvelles pour traiter les informations à caractère personnel » (97). S'il s'agit là d'un simple avis, dont le Conseil peut parfaitement s'abstraire, il va sans dire que l'arrêt *Marper* contraint en revanche le Conseil à revoir sa copie dans la direction indiquée, sauf, pour la future décision-cadre, à encourir une censure juridictionnelle. Encore faut-il savoir de quel juge...

2) En l'état actuel des voies de droit contentieuses ouvertes dans le troisième pilier de l'Union, le juge de Strasbourg est le mieux à même d'assurer la protection des données, fût-ce au moment du contrôle des actes nationaux d'exécution des différentes décisions-cadre en question.

On le sait, la compétence du juge communautaire, à l'heure actuelle, n'est que partielle voire absente pour tous les fichiers évoqués, les uns se rattachant au titre IV du T. CE en matière migratoire, les autres au troisième pilier, c'est-à-dire au titre VI du Traité UE relatif à la coopération policière et judiciaire en matière pénale (98). Les restrictions liées à la formation d'un recours en annulation sont ici bien connues (99), même dans le pilier communautaire et sans parler du troisième pilier. Certes une amélioration sensible est à attendre avec l'entrée en vigueur du Traité de Lisbonne, qui supprime les restrictions aux compétences de la Cour de Justice existant dans le cadre du titre IV Traité CE et du titre VI Traité UE, néanmoins une importante limitation subsiste en ce qui concerne la coopération policière et judiciaire en matière pénale, qui est celle de la clause d'ordre public de l'article 276 du Traité sur le fonctionnement de l'Union européenne (TFUE) (100).

Un paramètre important relativise cette crainte. Le considérant 25 de la proposition de décision-cadre relative au principe de disponibilité proclame expressément qu'elle « respecte les droits fondamentaux et observe les principes reconnus, en particulier, par la Charte des droits fondamentaux de l'Union ». De même, la décision-cadre sur la protection des données dans le troisième pilier (entrée quant à elle dans le droit positif) reprend cette même formule dans son considérant 48, et ajoute qu'elle « tend à préserver pleinement le droit au respect de la vie privée et le droit à la protection des données à caractère personnel consacrés aux articles 7 et 8 de la Charte ».

Un progrès majeur semble donc à espérer en matière de protection des données grâce à la Charte des droits fondamentaux de l'Union européenne aujourd'hui utilisée et demain justiciable. Si l'UE respecte de manière générale les droits fondamentaux, la Charte des droits fondamentaux, redécouverte par le Traité de Lisbonne - qui y fait référence dans son article 6 (101) - contient en effet une disposition spécifique relative à la protection des données à caractère personnel dans son art. 8 (102). Or l'article 6 du traité reconnaît désormais explicitement à la Charte la même valeur juridique que les traités, même si la Cour de Justice la prenait déjà largement en compte (103). Il reste à savoir si l'accès au prétoire communautaire sera suffisamment ouvert aux particuliers pour leur permettre de défendre ce droit à la protection des données tel que proclamé par la Charte, et ce dans toutes les circonstances, sur la base des progrès apportés par le Traité de Lisbonne en matière contentieuse pour les requérants individuels (104).

Il ressort de tout ce qui précède que le juge de Luxembourg n'est peut-être pas encore le mieux armé pour assurer la protection des données individuelles, soit que les textes ne lui donnent pas ou limitent sa compétence soit que le requérant ne puisse pas avoir accès au prétoire.

Au-delà, la soumission du droit de l'Union à la Conv. EDH et à sa jurisprudence ne pose pas problème. La jurisprudence *Bosphorus (105)* fait valoir l'intérêt du contrôle des mesures nationales d'exécution et laisse planer cette menace en cas de conflit. Si le droit de l'Union bénéficie d'une présomption de conformité à la Conv. EDH - formulée par la Cour européenne des droits de l'homme en des termes qui font inévitablement penser à la célèbre jurisprudence *Solange II* du Tribunal constitutionnel allemand (106) - cette présomption n'est pas irréfragable puisqu'elle peut « être renversée dans le cadre d'une affaire donnée si l'on estime que la protection des droits garantis par la Convention était entachée d'une insuffisance manifeste » (107). L'arrêt *Bosphorus*, en somme, ne fait qu'anticiper l'adhésion de l'UE à la Conv. EDH, prévue par l'art. 6 § 2 du nouveau traité UE (108), qui parachèvera la construction de l'édifice de la protection des droits fondamentaux en Europe, et il faut souligner d'ailleurs à quel point « les perspectives de l'adhésion à la Conv. EDH prévue par l'article 6 § 2 du Traité UE, pour lointaines qu'elles sont, ne modifient pas la pression qui s'établit d'ores et déjà sur le juge de l'Union » (109). Cette adhésion permettra d'attribuer un véritable statut contentieux à l'Union devant la Cour européenne des droits de l'homme, et, surtout, les particuliers bénéficieront du droit de recours individuel devant la Cour de Strasbourg pour contester tout acte de l'Union affectant leurs droits fondamentaux, alors même qu'ils n'auraient pas eu accès à la Cour de Justice pour les raisons évoquées plus haut.

Du reste, dans le domaine de la protection des données, la CJCE a elle-même reconnu la prééminence de la Convention européenne des droits de l'homme, dans l'affaire *Österreichische Rundfunk (110)*. Soulignant dans un premier temps que « les dispositions de la directive 95/46 en ce qu'elles régissent le traitement des données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante, font partie intégrante des principes généraux du droit dont la Cour assure le respect », et faisant ensuite expressément référence à l'article 8 de la Conv. EDH, elle a vérifié si la réglementation en cause prévoyait une ingérence dans la vie privée et si « le cas échéant, cette ingérence est justifiée au regard de l'article 8 de la Conv. EDH » en se référant à la jurisprudence suivie par la Cour européenne des droits de l'homme en la matière. D'ores et déjà, la Conv. EDH apparaît bien comme la référence en matière de protection des données. L'arrêt *Marper* fournit une arme de choix pour combattre les atteintes à la vie privée.

Au total, le juge de Strasbourg a bien l'essentiel des cartes en main pour suppléer aux carences législatives ou contentieuses de l'Union. L'arrêt rendu dans l'affaire *S. et Marper* prend à cet égard un relief considérable, car la Cour s'y

montre déterminée à assurer un contrôle scrupuleux en matière de protection des données à caractère personnel, l'arrêt ayant été rendu à l'unanimité, il convient de le rappeler. Au vu de la jurisprudence *Bosphorus*, mais aussi du rôle à jouer par la Cour de Justice - qui a déjà montré qu'elle prenait largement en compte la Conv. EDH et la jurisprudence de Strasbourg - le législateur de l'espace de liberté, sécurité et justice de l'Union européenne ne pourra pas ignorer les nouvelles règles du jeu édictées à Strasbourg. Cela donne à l'arrêt *Marper* une portée inaperçue au premier abord. Ainsi, après une période d'expansion de mesures sécuritaires dans un but de lutte contre la criminalité et le terrorisme, quitte à réduire l'espace de liberté comme peau de chagrin, le temps semble venu, grâce à l'arrêt *Marper*, d'un rééquilibrage au profit de la liberté des individus. Et c'est donc au juge de Strasbourg que revient en définitive le privilège de parachever la construction de l'espace de sécurité et de justice en y adjoignant le mot liberté.

Annexe

CEDH, gr. ch., 4 déc. 2008

***Affaires S. et Marper c/ Royaume-Uni*, req. n^{os} 30562/04 et 30566/04) (extraits)**

[...]

I. Sur la violation alléguée de l'article 8 de la convention

58. Les requérants se plaignent de la conservation, sur le fondement de l'article 64 § 1A de la loi de 1984 sur la police et les preuves en matière pénale (ci-après " la loi de 1984 "), de leurs empreintes digitales, échantillons cellulaires et profils génétiques. Ils y voient une violation de l'article 8.

A. Existence d'une ingérence dans la vie privée.

2. L'appréciation de la Cour

a. Principes généraux

66. La Cour rappelle que la notion de " vie privée " est une notion large, non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne (Pretty c. Royaume-Uni, no 2346/02, § 61, CEDH 2002 III, et Y.F. c. Turquie, no 24209/94, § 33, CEDH 2003 IX). Elle peut donc englober de multiples aspects de l'identité physique et sociale d'un individu (Mikuliç c. Croatie, n° 53176/99, § 53, CEDH 2002-I). Des éléments tels, par exemple, l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle relèvent de la sphère personnelle protégée par l'article 8 (voir, entre autres, Bensaid c. Royaume Uni, n° 44599/98, § 47, CEDH 2001 I et les références qui y sont citées, et Peck c. Royaume-Uni, n° 44647/98, § 57, CEDH 2003 I). Au-delà du nom, la vie privée et familiale peut englober d'autres moyens d'identification personnelle et de rattachement à une famille (voir, mutatis mutandis, Burghartz c. Suisse, 22 février 1994, § 24, série A n° 280 B, et Ünal Tekeli c. Turquie, n° 29865/96, § 42, CEDH 2004 X (extraits)). Les informations relatives à la santé d'une personne constituent un élément important de sa vie privée (Z c. Finlande, 25 février 1997, § 71, Recueil des arrêts et décisions 1997 I). La Cour estime de plus que l'identité ethnique d'un individu doit aussi être considérée comme un élément important de sa vie privée (voir notamment l'article 6 de la Convention sur la protection des données, cité au paragraphe 41 ci-dessus, qui fait entrer les données à caractère personnel révélant l'origine raciale, avec d'autres informations sensibles sur l'individu, parmi les catégories particulières de données ne pouvant être conservées que moyennant des garanties appropriées). L'article 8 protège en outre un droit à l'épanouissement personnel et celui de nouer et de développer des relations avec ses semblables et le monde extérieur (voir, par exemple, Burghartz, précité, avis de la Commission, p. 37, § 47, et Friedl c. Autriche, 31 janvier 1995, série A n° 305-B, avis de la Commission, p. 20, § 45). La notion de vie privée comprend par ailleurs des éléments se rapportant au droit à l'image (Sciacca c. Italie, n° 50774/99, § 29, CEDH 2005 I).

67. Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 (Leander c. Suède, 26 mars 1987, § 48, série A n° 116). Peu importe que les informations mémorisées soient ou non utilisées par la suite (Amann c. Suisse [GC], n° 27798/95, § 69, CEDH 2000 II). Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu l'un des aspects de la vie privée précités, la Cour tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés (voir, mutatis mutandis, Friedl, précité, avis de la Commission, §§ 49-51, et Peck c. Royaume-Uni, précité, § 59).

b. Application des principes précités au cas d'espèce

68. La Cour note d'emblée que les trois catégories d'informations personnelles conservées par les autorités au sujet des deux requérants, à savoir des empreintes digitales, des profils ADN et des échantillons cellulaires, constituent toutes des données à caractère personnel au sens de la Convention sur la protection des données car elles se rapportent à des individus identifiés ou identifiables. Le Gouvernement admet de son côté que dans les trois cas il s'agit de « données à caractère personnel », au sens de la loi de 1998 sur la protection des données, qui se trouvent entre les mains de personnes en mesure d'identifier les individus concernés.

69. Les organes de la Convention se sont déjà penchés à diverses reprises, dans le contexte de procédures pénales, sur des questions se rapportant à la conservation par les autorités de telles données à caractère personnel. Pour ce qui est de la nature et de la portée des informations contenues dans chacune des trois catégories de données, la Cour a par le passé établi une distinction entre la conservation des empreintes digitales et celle des échantillons cellulaires et profils ADN au motif que les informations personnelles contenues dans ces deux dernières catégories se prêtent davantage à des utilisations ultérieures (Van der Velden c. Pays-Bas (déc.), n° 29514/05, CEDH 2006 ...). Elle estime en l'espèce que la question de l'atteinte au droit des requérants au respect de leur vie privée doit être examinée séparément pour la conservation de leurs échantillons cellulaires et profils ADN et pour celle de leurs empreintes digitales.

i. Les échantillons cellulaires et profils ADN

70. Dans l'affaire Van der Velden, a Cour a estimé que, vu les usages futurs que l'on pouvait envisager notamment pour les échantillons cellulaires, la conservation systématique de pareils éléments était suffisamment intrusive pour entraîner une atteinte au droit au respect de la vie privée. Le Gouvernement a critiqué cette conclusion, arguant qu'elle reposait sur des hypothèses quant aux utilisations qui pourraient être faites des échantillons à l'avenir et qu'il n'y avait rien de tel dans l'immédiat.

71. La Cour réaffirme son opinion selon laquelle les préoccupations d'un individu quant aux utilisations susceptibles d'être faites à l'avenir d'informations privées conservées par les autorités sont légitimes et pertinentes pour la question de savoir s'il y a eu ou non ingérence. De fait, compte tenu du rythme élevé auquel se succèdent les innovations dans le domaine de la génétique et des technologies de l'information, la Cour ne peut écarter la possibilité que les aspects de la vie privée se rattachant aux informations génétiques fassent à l'avenir l'objet d'atteintes par des voies nouvelles, que l'on

ne peut prévoir aujourd'hui avec précision. Dès lors, la Cour n'aperçoit aucune raison justifiant qu'elle s'écarte de la conclusion à laquelle elle est parvenue dans l'affaire Van der Velden.

72. Toutefois, les préoccupations légitimes quant aux usages susceptibles d'être faits des échantillons cellulaires à l'avenir ne sauraient être le seul élément à prendre en compte pour trancher la question qui se pose. En dehors de leur caractère éminemment personnel, la Cour note que les échantillons cellulaires contiennent beaucoup d'informations sensibles sur un individu, notamment sur sa santé. De surcroît, les échantillons renferment un code génétique unique qui revêt une grande importance tant pour la personne concernée que pour les membres de sa famille. À cet égard, la Cour souscrit à l'opinion exprimée par la baronne Hale lors de la procédure devant la Chambre des lords (paragraphe 25 ci-dessus).

73. Vu la nature et la quantité des informations personnelles contenues dans les échantillons cellulaires, leur conservation doit passer pour constituer en soi une atteinte au droit au respect de la vie privée des individus concernés. Peu importe que seule une petite partie de ces informations soit en réalité extraite ou utilisée par les autorités pour les besoins de la création de profils ADN et qu'aucun préjudice immédiat ne soit provoqué dans un cas particulier (Amann, précité, § 69).

74. Pour ce qui est des profils ADN, la Cour relève qu'ils contiennent moins d'informations personnelles. Extraites des échantillons cellulaires, celles-ci se présentent sous la forme d'un code. Le Gouvernement soutient qu'un profil ADN n'est rien de plus qu'une séquence de chiffres ou un code-barres contenant des informations purement objectives et irréfutables et que l'identification d'une personne ne se produit qu'en cas de concordance avec un profil contenu dans la base de données. Il déclare aussi que, les informations en question étant codées, il faut recourir à la technologie informatique pour les rendre intelligibles et que seul un nombre restreint de personnes seraient en mesure de les interpréter.

75. La Cour observe néanmoins que les profils contiennent une quantité importante de données à caractère personnel uniques. Même si les informations contenues dans les profils peuvent passer pour objectives et irréfutables au sens où l'entend le Gouvernement, leur traitement automatisé permet aux autorités d'aller bien au-delà d'une identification neutre. Elle note à cet égard que, de l'aveu même du Gouvernement, les profils ADN peuvent être utilisés - et l'ont été dans certains cas - pour effectuer des recherches familiales en vue de déceler un éventuel lien génétique entre des individus. Le Gouvernement reconnaît aussi le caractère hautement sensible de ce type de recherches et la nécessité d'exercer des contrôles très stricts en la matière. Selon la Cour, le fait que les profils ADN fournissent un moyen de découvrir les relations génétiques pouvant exister entre des individus (paragraphe 39 ci-dessus) suffit en soi pour conclure que leur conservation constitue une atteinte au droit à la vie privée de ces individus. La fréquence des recherches familiales, les garanties qui les entourent et la probabilité que survienne un préjudice dans un cas donné importent peu à cet égard (Amann, précité, § 69). De même, le fait que, l'information étant codée, elle ne soit intelligible qu'à l'aide de l'informatique et ne puisse être interprétée que par un nombre restreint de personnes ne change rien à cette conclusion.

76. La Cour relève par ailleurs que le Gouvernement ne conteste pas que le traitement des profils ADN permette aux autorités de se faire une idée de l'origine ethnique probable du donneur et que cette technique est effectivement utilisée dans le cadre des enquêtes policières (paragraphe 40 ci-dessus). La possibilité qu'offrent les profils ADN de tirer des déductions quant à l'origine ethnique rend leur conservation d'autant plus sensible et susceptible de porter atteinte au droit à la vie privée. Cette conclusion cadre avec la Convention sur la protection des données et la loi sur la protection des données, qui en est le reflet, ces deux textes classant les données à caractère personnel révélant l'origine ethnique parmi les catégories particulières de données appelant une protection accrue (paragraphes 30-31 et 41 ci-dessus).

73. Dans ces conditions, la Cour conclut que la conservation tant des échantillons cellulaires que des profils ADN des requérants s'analyse en une atteinte au droit de ces derniers au respect de leur vie privée au sens de l'article 8 § 1 de la Convention.

ii. Les empreintes digitales

78. Il est constant que les empreintes digitales ne contiennent pas autant d'informations que les échantillons cellulaires ou les profils ADN. La question de l'impact de leur conservation par les autorités sur le droit au respect de la vie privée a déjà été étudiée par les organes de la Convention.

79. C'est la Commission qui, dans l'affaire McVeigh, s'est penchée pour la première fois sur la question du prélèvement et de la conservation d'empreintes digitales. Celles en cause dans ladite affaire avaient été prélevées dans le cadre d'une série de mesures d'enquête. La Commission admit que certaines de ces mesures au moins avaient porté atteinte au droit des requérants au respect de leur vie privée, mais elle ne trancha pas le point de savoir si la conservation des empreintes digitales aurait à elle seule été constitutive de pareille atteinte (McVeigh, O'Neill et Evans, nos 8022/77, 8025/77 et 8027/77, rapport de la Commission du 18 mars 1981, DR 25, p. 93, § 224).

80. Dans l'affaire Kinnunen, la Commission considéra que la conservation après l'arrestation du requérant de ses empreintes digitales et photographies ne s'analysait pas en une ingérence dans sa vie privée dès lors que ces éléments ne contenaient aucune appréciation subjective sujette à contestation. La Commission nota toutefois que les données en question avaient été détruites neuf ans plus tard à la demande du requérant (Kinnunen c. Finlande, n° 24950/94, décision de la Commission du 15 mai 1996).

81. Eu égard à ces conclusions et aux questions que soulève la présente affaire, la Cour estime qu'il convient de réexaminer le problème. Elle note d'emblée que les empreintes digitales numérisées des requérants constituent des données à caractère personnel les concernant (paragraphe 68 ci-dessus) et qu'elles contiennent certains traits externes d'identification, tout comme, par exemple, des photographies ou des échantillons de voix.

82. Dans l'affaire Friedl, la Commission considéra que la conservation de photographies anonymes prises lors d'une manifestation publique ne s'analysait pas en une ingérence dans la vie privée. Elle parvint à cette conclusion en accordant un poids particulier au fait que les photographies en question n'avaient été enregistrées dans aucun système de traitement de données et que les autorités n'avaient pas pris de mesures pour identifier les personnes photographiées en recourant au traitement de données (Friedl, précité, avis de la Commission, §§ 49-51).

83. Dans l'affaire P.G. et J.H., la Cour a quant à elle estimé que l'enregistrement de données et le caractère systématique ou permanent de l'enregistrement était susceptible de faire entrer en jeu le droit au respect de la vie privée même si les données concernées étaient dans le domaine public ou disponibles d'une autre manière. Elle a observé que l'enregistrement de la voix d'une personne sur un support permanent en vue d'une analyse ultérieure était manifestement de nature, combiné à d'autres données personnelles, à faciliter l'identification de cette personne. Elle a donc jugé que l'enregistrement des voix des requérants en vue d'une telle analyse ultérieure avait porté atteinte à leur droit au respect de leur vie privée (P.G. et J.H. c. Royaume-Uni, n° 44787/98, §§ 59-60, CEDH 2001 IX).

84. La Cour considère que l'approche adoptée par les organes de la Convention au sujet des photographies et

échantillons de voix doit aussi être appliquée aux empreintes digitales. Le Gouvernement estime que ces dernières constituent un cas à part au motif qu'il s'agirait d'éléments neutres, objectifs et irréfutables qui, contrairement aux photographies, ne seraient pas intelligibles pour un oeil non exercé et en l'absence d'autres empreintes avec lesquelles les comparer. Certes, mais cela ne change rien au fait que les empreintes digitales contiennent objectivement des informations uniques sur l'individu concerné et permettent une identification précise dans un grand nombre de circonstances. Les empreintes digitales sont donc susceptibles de porter atteinte à la vie privée, et leur conservation sans le consentement de l'individu concerné ne saurait passer pour une mesure neutre ou banale.

85. Dès lors, la Cour estime que la conservation, dans les fichiers des autorités, des empreintes digitales d'un individu identifié ou identifiable peut en soi donner lieu, en dépit du caractère objectif et irréfutable de ces données, à des préoccupations importantes concernant le respect de la vie privée.

86. En l'espèce, la Cour note en outre que les empreintes digitales des requérants ont 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. Chacun admet à cet égard que, de par les informations que les échantillons cellulaires et profils ADN contiennent, la conservation de ces éléments a un impact plus grand sur la vie privée que celle d'empreintes digitales. Toutefois, à l'instar de la baronne Hale (paragraphe 25 ci-dessus), la Cour estime que, s'il peut se révéler nécessaire de distinguer entre les empreintes digitales, d'une part, et les échantillons et profils, d'autre part, pour ce qui est de leur prélèvement, de leur utilisation et de leur stockage lorsqu'il s'agit de trancher la question de la justification, il n'en demeure pas moins que la conservation d'empreintes digitales constitue une atteinte au droit au respect de la vie privée.

B. Justification de l'ingérence [...]

2. L'appréciation de la Cour

a. Prévue par la loi

95. La Cour rappelle sa jurisprudence constante selon laquelle les termes " prévue par la loi " signifient que la mesure litigieuse doit avoir une base en droit interne et être compatible avec la prééminence du droit, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8. La loi doit ainsi être suffisamment accessible et prévisible, c'est-à-dire énoncée avec assez de précision pour permettre à l'individu - en s'entourant au besoin de conseils éclairés - de régler sa conduite. Pour que l'on puisse la juger conforme à ces exigences, elle doit fournir une protection adéquate contre l'arbitraire et, en conséquence, définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes (Malone c. Royaume-Uni, 2 août 1984, §§ 66-68, série A n° 82, Rotaru c. Roumanie [GC], n° 28341/95, § 55, CEDH 2000 V, et Amann, précité, § 56).

96. Le niveau de précision requis de la législation interne - laquelle ne peut du reste parer à toute éventualité - dépend dans une large mesure du contenu du texte considéré, du domaine qu'il est censé couvrir et du nombre et de la qualité de ses destinataires (Hassan et Tchaouch c. Bulgarie [GC], n° 30985/96, § 84, CEDH 2000 XI, et références citées).

97. La Cour relève que, en vertu de l'article 64 de la loi de 1984, les empreintes digitales ou échantillons pris sur une personne dans le cadre de l'enquête sur une infraction peuvent être conservés une fois qu'ils ont été employés dans le but prévu (paragraphe 27 ci-dessus). La Cour convient avec le Gouvernement que la conservation des empreintes digitales, des échantillons biologiques et des profils génétiques des requérants avait ainsi à l'évidence une base en droit interne. Il apparaît aussi clairement que, sauf circonstances exceptionnelles, ces éléments sont en pratique conservés. Le fait que les commissaires de police aient le pouvoir de les détruire dans des cas exceptionnels ne rend pas la loi insuffisamment précise du point de vue de la Convention.

98. Pour ce qui est des conditions et des modalités de mémorisation et d'utilisation de ces informations personnelles, l'article 64 est en revanche beaucoup moins précis. Il dispose que les échantillons et empreintes digitales conservés ne doivent pas être utilisés par quiconque, sauf à des fins en rapport avec la prévention ou la détection des infractions pénales, l'enquête sur une infraction ou la conduite de poursuites.

99. La Cour convient avec les requérants que le premier au moins de ces objectifs est exprimé en termes assez généraux et se prête à une interprétation très large. Elle rappelle que, dans ce contexte comme dans celui des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire (voir, mutatis mutandis, Kruslin c. France, 24 avril 1990, §§ 33 et 35, série A n° 176 A, Rotaru, précité, §§ 57-59, Weber et Saravia c. Allemagne (déc.), n° 54934/00, CEDH 2006 ..., Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie, n° 62540/00, §§ 75-77, 28 juin 2007, Liberty et autres c. Royaume-Uni, n° 58243/00, §§ 62-63, 1er juillet 2008). La Cour note cependant que ces aspects sont en l'espèce étroitement liés à la question plus large de la nécessité de l'ingérence dans une société démocratique. Compte tenu de l'analyse à laquelle elle s'est livrée aux paragraphes 105 à 126 ci-dessous, la Cour juge qu'il n'y a pas lieu de trancher le point de savoir si le libellé de l'article 64 répond aux exigences quant à la " qualité " de la loi, au sens de l'article 8 § 2 de la Convention.

b. But légitime

100. La Cour admet avec le Gouvernement que la conservation des données relatives aux empreintes digitales et génétiques vise un but légitime : la détection et, par voie de conséquence, la prévention des infractions pénales. Alors que le prélèvement initial est destiné à relier une personne donnée à l'infraction particulière qu'elle est soupçonnée d'avoir commise, la conservation tend à un objectif plus large, à savoir contribuer à l'identification des futurs délinquants.

c. Nécessaire dans une société démocratique

i. Principes généraux

101. Une ingérence est considérée comme " nécessaire dans une société démocratique " pour atteindre un but légitime si elle répond à un " besoin social impérieux " et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent " pertinents et suffisants ". S'il appartient aux autorités nationales de juger les premières si toutes ces conditions se trouvent remplies, c'est à la Cour qu'il revient de trancher en définitive la question de la nécessité de l'ingérence au regard des exigences de la Convention (Coster c. Royaume-Uni [GC], n° 24876/94, § 104, 18 janvier 2001, et références citées).

102. Il faut reconnaître à cet égard une certaine marge d'appréciation aux autorités nationales compétentes. L'étendue de cette marge est variable et dépend d'un certain nombre de facteurs, dont la nature du droit en cause garanti par la Convention, son importance pour la personne concernée, la nature de l'ingérence et la finalité de celle-ci. Cette marge est

d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre " intime " qui lui sont reconnus (Connors c. Royaume-Uni, n° 66746/01, § 82, 27 mai 2004, et références citées). Lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, la marge laissée à l'Etat est restreinte (Evans c. Royaume-Uni [GC], n° 6339/05, § 77, CEDH 2007 ...). En revanche, lorsqu'il n'y a pas de consensus au sein des Etats membres du Conseil de l'Europe, que ce soit sur l'importance relative de l'intérêt en jeu ou sur les meilleurs moyens de le protéger, la marge d'appréciation est plus large (Dickson c. Royaume-Uni [GC], n° 44362/04, § 78, CEDH 2007 ...).

103. La protection des données a? caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données a? caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (voir, mutatis mutandis, Z c. Finlande, précité, § 95). 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. Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (préambule et article 5 de la Convention sur la protection des données et principe 7 de la recommandation R(87)15 du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police). Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (voir notamment l'article 7 de la Convention sur la protection des données). Les considérations qui précèdent valent tout spécialement lorsqu'est en jeu la protection de catégories particulières de données plus sensibles (article 6 de la Convention sur la protection des données), notamment des données ADN, qui, dans la mesure où elles contiennent le patrimoine génétique de la personne, revêtent une grande importance tant pour elle-même que pour sa famille (recommandation No R (92) 1 du Comité des Ministres sur l'utilisation des analyses de l'ADN dans le cadre du système de justice pénale).

104. 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 (article 9 de la Convention sur la protection des données). Cependant, compte tenu du caractère intrinsèquement privé de ces informations, la Cour se doit de procéder à un examen rigoureux de toute mesure prise par un Etat pour autoriser leur conservation et leur utilisation par les autorités sans le consentement de la personne concernée (voir, mutatis mutandis, Z c. Finlande, précité, § 96).

ii. Application de ces principes au cas d'espèce

105. Pour la Cour, il est hors de doute que la lutte contre la criminalité, et notamment contre le crime organisé et le terrorisme, qui constitue l'un des défis auxquels les sociétés européennes doivent faire face à l'heure actuelle, dépend dans une large mesure de l'utilisation des techniques scientifiques modernes d'enquête et d'identification. Le Conseil de l'Europe a reconnu il y a plus de quinze ans que les techniques d'analyse de l'ADN présentaient des avantages pour le système de la justice pénale (recommandation R (92) 1 du Comité des Ministres, paragraphes 43-44 ci dessus). Il est constant, par ailleurs, que les Etats membres ont depuis lors réalisé des progrès rapides et substantiels en matière d'utilisation des données ADN pour établir l'innocence ou la culpabilité.

106. Néanmoins, tout en reconnaissant le rôle important que jouent ces informations dans la détection des infractions, la Cour doit délimiter la portée de son examen. La question n'est pas de déterminer si la conservation des empreintes digitales, échantillons cellulaires et profils ADN en général peut passer pour justifiée au regard de la Convention. Le seul point sur lequel la Cour doive se pencher est celui 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, se justifiait sous l'angle de l'article 8 § 2 de la Convention.

107. La Cour procédera à son examen en tenant dûment compte des instruments pertinents du Conseil de l'Europe et du droit et de la pratique en vigueur dans les autres Etats contractants. D'après les principes clés en la matière, la conservation des données doit être proportionnée au but pour lequel elles ont été recueillies et être limitée dans le temps (paragraphes 41-44 ci-dessus). Il apparaît que les Etats contractants appliquent systématiquement ces principes dans le secteur de la police, conformément à la Convention sur la protection des données et aux recommandations ultérieures du Comité des Ministres (paragraphes 45-49 ci-dessus).

108. Pour ce qui concerne plus particulièrement les échantillons cellulaires, la plupart des Etats contractants n'en autorisent le prélèvement dans le cadre de procédures pénales que sur les individus soupçonnés d'avoir commis des infractions présentant un certain seuil de gravité. Dans la grande majorité des Etats contractants disposant de bases de données ADN en service, les échantillons et les profils génétiques qui en sont tirés doivent être respectivement détruits ou effacés soit immédiatement soit dans un certain délai après un acquittement ou un non-lieu. Certains Etats contractants autorisent un nombre restreint d'exceptions à ce principe (paragraphes 47-48 ci-dessus).

109. La situation qui prévaut actuellement en Ecosse, qui fait partie du Royaume-Uni, est à cet égard particulièrement significative. Comme indiqué plus haut (paragraphe 36), le Parlement écossais a autorisé la conservation de l'ADN de personnes non condamnées uniquement pour les adultes accusés d'infractions violentes ou d'infractions sexuelles et, même dans ce cas, pour une durée de trois ans seulement, avec la possibilité de conserver ces éléments pendant deux années supplémentaires avec l'accord d'un sheriff.

110. Cette situation est conforme à la recommandation R (92) 1 du Comité des Ministres, qui insiste sur la nécessité d'établir des distinctions entre les différents types de cas et d'appliquer des durées précises de conservation des données, même dans les cas les plus graves (paragraphes 43-44 ci-dessus). En réalité, l'Angleterre, le pays de Galles et l'Irlande du Nord sont 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.

111. Le Gouvernement insiste sur le fait que le Royaume-Uni est à l'avant-garde pour ce qui est du développement de l'usage des échantillons d'ADN en vue de la détection des infractions pénales et que les autres Etats ne sont pas parvenus à la même maturité en ce qui concerne la taille et les ressources de leurs bases de données ADN. Selon lui, l'analyse comparative du droit et de la pratique en vigueur dans les autres Etats ne revêt donc qu'un intérêt limité.

112. La Cour ne peut toutefois ignorer le fait que, en dépit des avantages susceptibles de découler d'un élargissement maximal de la base de données ADN, d'autres Etats contractants ont décidé de fixer des limites à la conservation et à l'utilisation de telles données afin de parvenir à un équilibre adéquat avec l'intérêt concurrent que constitue la préservation de la vie privée. Elle observe que la protection offerte par l'article 8 de la Convention 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. Pour la Cour, le

fort consensus qui existe à cet égard au sein des Etats contractants revêt une importance considérable et réduit la marge d'appréciation dont l'Etat défendeur dispose pour déterminer jusqu'où peut aller l'ingérence dans la vie privée permise dans ce domaine. La Cour considère que tout Etat qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière.

113. En l'espèce, les empreintes digitales et échantillons cellulaires des requérants ont été prélevés et leurs profils ADN réalisés dans le cadre de procédures pénales engagées pour tentative de vol dans le cas du premier requérant et pour harcèlement à l'égard de sa compagne dans le cas du second. Les données ont été stockées sur la base d'une loi autorisant leur conservation pour une durée illimitée, alors même que le premier requérant a été acquitté et que le second a vu son affaire classée sans suite.

114. La Cour doit examiner si la conservation permanente des empreintes digitales et données ADN de toutes les personnes soupçonnées mais non condamnées se fonde sur des motifs pertinents et suffisants.

115. Bien que le pouvoir de conserver les empreintes digitales, échantillons cellulaires et profils ADN de personnes non condamnées n'existe en Angleterre et aux pays de Galles que depuis 2001, le Gouvernement estime qu'il est démontré que la conservation de ces éléments est indispensable dans le cadre de la lutte contre la criminalité. Et de fait, les statistiques et autres éléments de preuve soumis à la Chambre des lords et repris dans les documents présentés à la Cour par le Gouvernement (paragraphe 92 ci-dessus) apparaissent impressionnants, dans la mesure où ils indiquent que des profils ADN qui auraient auparavant été détruits ont été reliés à des traces relevées sur les lieux d'infractions dans un nombre élevé de cas.

116. Les requérants soutiennent toutefois que ces statistiques sont trompeuses, point de vue que confirme le rapport Nuffield. En effet, comme les requérants le font remarquer, les chiffres n'indiquent pas dans quelle mesure ce " lien " avec des traces recueillies sur les lieux d'infractions a conduit à la condamnation des personnes concernées, ni le nombre de condamnations dues à la conservation des échantillons de personnes non condamnées. Ils ne prouvent pas non plus que le fort taux de concordance avec des traces provenant de lieux d'infractions n'ait été rendu possible que grâce à la conservation illimitée des éléments ADN de toutes ces catégories de personnes. Parallèlement, dans la majorité des cas précis cités par le Gouvernement (paragraphe 93 ci-dessus), les données ADN tirées des prélèvements effectués sur des suspects ont uniquement débouché sur des correspondances avec des traces antérieures conservées dans la base de données. Or ces correspondances auraient pu être établies même en l'absence du dispositif actuel, qui autorise la conservation illimitée des données ADN de tous les individus soupçonnés mais non condamnés.

117. Tout en observant que ni les statistiques ni les exemples fournis par le Gouvernement ne permettent en eux-mêmes d'établir qu'il serait impossible d'identifier et de poursuivre avec succès les auteurs d'infractions sans la conservation permanente et indifférenciée des empreintes digitales et données ADN de toutes les personnes se trouvant dans une situation analogue à celle des requérants, la Cour admet que l'élargissement de la base de données a contribué à la détection et à la prévention des infractions pénales.

118. Il reste toutefois à déterminer si pareille conservation est proportionnée et reflète un juste équilibre entre les intérêts publics et privés qui se trouvent en concurrence.

119. A cet égard, la Cour est frappée par le caractère général et indifférencié du pouvoir de conservation en vigueur en Angleterre et au pays de Galles. En effet, les données en cause peuvent 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 ; il est possible de prélever - puis de les conserver - des empreintes digitales et des échantillons biologiques chez toute personne, quel que soit son âge, arrêtée en rapport avec une infraction emportant inscription dans les fichiers de la police, étant entendu que des infractions mineures ou non punies d'une peine d'emprisonnement peuvent donner lieu à pareille inscription. Par ailleurs, la conservation n'est pas limitée dans le temps : les éléments sont conservés indéfiniment, indépendamment de la nature ou de la gravité de l'infraction que la personne est soupçonnée d'avoir commise. De plus, il n'existe que peu de possibilités pour un individu acquitté d'obtenir l'effacement des données de la base nationale ou la destruction des échantillons (paragraphe 35 ci-dessus) ; en particulier, le législateur n'a pas prévu l'exercice d'un contrôle indépendant de la justification de la conservation sur la base de critères précis, tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière.

120. La Cour reconnaît que l'atteinte au droit des requérants au respect de leur vie privée peut être d'un degré différent pour chacune des trois catégories de données à caractère personnel conservées. La conservation d'échantillons cellulaires est particulièrement intrusive, compte tenu de la profusion d'informations génétiques et relatives à la santé qu'ils contiennent. Cela étant, un régime de conservation aussi indifférencié et inconditionné que celui en cause exige de procéder à un examen rigoureux sans tenir compte de ces différences.

121. Le Gouvernement plaide que la conservation ne pourrait avoir un effet direct ou important sur les requérants que si des correspondances établies avec la base de données venaient à l'avenir à révéler leur implication dans des infractions. La Cour ne peut souscrire à cet argument. Elle réaffirme que le simple fait de la conservation ou de la mémorisation de données à caractère personnel par les autorités publiques, quelle que soit la manière dont celles-ci ont été obtenues, doit passer pour emporter des conséquences directes sur la vie privée de l'individu concerné, que ces données soient utilisées par la suite ou non (paragraphe 67 ci-dessus).

122. Particulièrement préoccupant en l'occurrence est le risque de stigmatisation, qui découle du fait que les personnes dans la situation des requérants, qui n'ont été reconnus coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence, sont traitées de la même manière que des condamnés. Il convient de ne pas perdre de vue à cet égard que le droit de toute personne à être présumée innocente que garantit la Convention comporte une règle générale en vertu de laquelle on ne peut plus exprimer des soupçons sur l'innocence d'un accusé une fois que celui-ci a été acquitté (Rushiti c. Autriche, n° 28389/95, § 31, 21 mars 2000, et références citées). Certes, la conservation de données privées concernant les requérants n'équivaut pas à l'expression de soupçons. Néanmoins, l'impression qu'ont les intéressés de ne pas être considérés comme innocents se trouve renforcée par le fait que les données les concernant sont conservées indéfiniment tout comme celles relatives à des personnes condamnées, alors que celles concernant des individus n'ayant jamais été soupçonnés d'une infraction doivent être détruites.

123. Le Gouvernement argue que le pouvoir de conservation s'applique à l'ensemble des empreintes digitales et échantillons biologiques prélevés sur une personne dans le cadre d'une enquête sur une infraction et ne dépend pas de l'innocence ou de la culpabilité. De surcroît, les empreintes digitales et échantillons prélevés sur les requérants l'auraient été légalement et leur conservation ne serait pas liée au fait que les intéressés ont à l'origine été soupçonnés d'une infraction mais découlerait du seul souci d'augmenter la taille et donc l'usage de la base de données en vue de l'identification de criminels à l'avenir. La Cour juge toutefois que cet argument se concilie difficilement avec l'obligation, prévue à l'article 64 § 3 de la loi de 1984, de détruire, à leur demande, les empreintes digitales et échantillons des personnes s'étant soumises volontairement à des prélèvements, ces éléments ayant tout autant de valeur pour l'augmentation de la taille et de l'utilité de la base de données. Il faudrait que le Gouvernement avance de puissantes raisons pour que la Cour puisse estimer justifiée une telle différence de traitement entre les données personnelles des requérants et celles d'autres personnes non condamnées.

124. La Cour estime en outre que la conservation de données relatives à des personnes non condamnées peut être particulièrement préjudiciable dans le cas de mineurs, tel le premier requérant, en raison de leur situation spéciale et de l'importance que revêt leur développement et leur intégration dans la société. La Cour a déjà insisté, en s'inspirant des dispositions de l'article 40 de la Convention des Nations unies sur les droits de l'enfant de 1989, sur la place particulière qu'occupent les jeunes gens dans le domaine de la justice pénale, et elle a notamment souligné la nécessité de protéger leur vie privée dans le contexte des procédures pénales (T. c. Royaume-Uni [GC], n° 24724/94, §§ 75 et 85, 16 décembre 1999). De la même manière, la Cour considère qu'il faut veiller avec un soin particulier à protéger les mineurs de tout préjudice qui pourrait résulter de la conservation par les autorités, après un acquittement, des données privées les concernant. La Cour partage l'avis du Nuffield Council quant aux conséquences pour les jeunes gens d'une conservation illimitée de leurs échantillons et profils ADN et prend note des préoccupations exprimées par cet organisme au sujet de la surreprésentation dans la base de données des mineurs et des membres de minorités ethniques n'ayant été reconnus coupables d'aucune infraction à laquelle les politiques suivies aurait conduit (paragraphes 38-40 ci-dessus).

125. En conclusion, la Cour estime 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 traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'Etat défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique. Cette conclusion dispense la Cour d'examiner les critiques formulées par les requérants à l'encontre de certains points précis du régime de conservation des données litigieuses, tels l'accès, trop large selon eux, à ces données et la protection, insuffisante à leurs yeux, offerte contre les usages impropres ou abusifs de ces données.

126. Dès lors, il y a eu en l'espèce violation de l'article 8 de la Convention.

II. Sur la violation alléguée de l'article 14 combiné avec l'article 8 de la convention

127. Les requérants allèguent qu'ils ont été soumis à un traitement discriminatoire par rapport aux autres personnes se trouvant dans une situation analogue, c'est-à-dire aux personnes non condamnées dont les échantillons doivent toujours être détruits en vertu de la législation. Ce traitement découlerait de leur situation et relèverait de l'article 14, qui aurait toujours été interprété avec souplesse. Pour les motifs exposés sur le terrain de l'article 8, ce traitement serait dépourvu de justification raisonnable et objective, il ne viserait aucun but légitime et il ne présenterait pas un rapport de proportionnalité raisonnable avec le but affiché - la prévention des infractions - notamment pour ce qui est des échantillons, lesquels ne joueraient aucun rôle dans la détection ou la prévention des infractions pénales. Conserver des éléments concernant des personnes censées bénéficier de la présomption d'innocence, ce serait opérer une distinction de traitement totalement injustifiée et préjudiciable.

128. Le Gouvernement soutient pour sa part que l'article 14 est inapplicable faute pour l'article 8 d'entrer en jeu. Il ajoute que, quand bien même l'article 14 serait applicable, il n'existerait pas de différence de traitement, toutes les personnes dans une situation analogue à celle des requérants étant traitées de la même manière et les requérants ne pouvant se comparer aux individus n'ayant pas eu à se soumettre à un prélèvement d'échantillons par la police ou à ceux s'étant volontairement soumis à pareil prélèvement. En tout état de cause, la différence de traitement alléguée par les intéressés ne se fonderait pas sur une " situation " ou une caractéristique personnelle mais sur un fait historique. A supposer qu'il y eût une quelconque différence de traitement, elle serait objectivement justifiée et relèverait de la marge d'appréciation de l'Etat.

129. La Cour renvoie à sa conclusion ci-dessus selon laquelle la conservation des empreintes digitales, échantillons cellulaires et profils ADN des requérants a emporté violation de l'article 8 de la Convention. A la lumière du raisonnement qui a conduit à ce constat, elle considère qu'il n'y a pas lieu d'examiner séparément le grief tiré par les requérants de l'article 14 de la Convention.

Par ces motifs, la cour, à l'unanimité,

1. Dit qu'il y a eu violation de l'article 8 de la Convention ;

2. Dit qu'il n'y a pas lieu d'examiner séparément le grief tiré de l'article 14 de la Convention ;

3. Dit que le constat d'une violation fournit en soi une satisfaction équitable suffisante pour le dommage moral subi par les requérants.

Mots clés :
INFORMATIQUE * Donnée nominative * Fichier de police * Acquittement
DROIT ET LIBERTE FONDAMENTAUX * Vie privée et familiale * Donnée personnelle * Fichier de police * Acquittement
POLICE * Généralités * Fichier de police * Donnée nominative * Acquittement

(1) V. Thomas Hammarberg, Commissaire européen aux droits de l'homme, rapport du 10 déc. 2008, Lutte contre le terrorisme et protection du droit au respect de la vie privée, CommDH/IssuePaper (2008)3.

(2) Req. n° 30562/04 et 30566/04.

(3) V. Question orale avec débat, posée au Parlement européen le 9 décembre 2008, par Baroness Sarah Ludford et Alexander Alvaro, au nom du groupe ALDE, au Conseil et à la Commission, réf. 0-0136/08 et 0-0137/08.

(4) V. § 125 de l'arrêt.

(5) Programme de La Haye, adopté par le Conseil européen de Bruxelles du 4 novembre 2004, conclusions de la Présidence 8 décembre 2004, 14292/1/04.

(6) V. le rapport de T. Hammarberg, préc. (§ 5.3).

(7) Échantillons cellulaires et profils génétiques.

(8) À noter que la Cour, soulignant que l'identité ethnique d'un individu doit aussi être considérée comme un élément important de sa vie privée, fait plus spécifiquement référence à l'art. 6 de la Convention sur la protection des données, Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ou Convention 108 ; elle y avait déjà fait référence dans l'arrêt *Amann c/*

Suisse du 16 février 2000 (req. n° 27798/95, v. *Les grands arrêts de la Cour européenne des droits de l'homme*, F. Sudre, J.P. Marguénaud, J. Andriantsimbazovina, A. Gouttenoire, M. Levinet, PUF, 5e éd., janv. 2009, p. 433) en citant ses art. 1 et 2, qui sont au coeur de notre sujet ; l'art. 1 garantit le droit au respect de la vie privée à l'égard du traitement automatisé des données à caractère personnel la concernant ; l'art. 2 définit ces dernières comme « toute information concernant une personne physique identifiée ou identifiable ».

(9) La Cour estime que la notion de vie privée recouvre : l'intégrité physique et morale de la personne (*Pretty c/ Royaume-Uni*, req. n° 2346/02) ; l'identité physique et sociale d'un individu (*Mikulic c/ Croatie*, req. n° 53176/99 ; l'identité sexuelle, le nom, l'orientation sexuelle et la vie sexuelle (*Bensaïd c/ Royaume-Uni*, req. n° 44599/98) ; les informations relatives à la santé (*Z. c/ Finlande*, 25 févr. 1997, v. GACEDH, p. 444) ; ou encore le droit à l'épanouissement personnel et celui de nouer et de développer des relations avec ses semblables et le monde extérieur (*Burghartz*, 22 févr. 1994, v. GACEDH, p. 452).

(10) CEDH 26 mars 1987, *Leander c/ Suède*, req. n° 9248/81, v. GACEDH, p. 446 ; v. § 48 : « le registre secret de la police renfermait sans contredit des données relatives à la vie privée de M. Leander. Tant leur mémorisation que leur communication, assorties du refus d'accorder à M. Leander la faculté de les réfuter, portaient atteinte à son droit au respect de sa vie privée, garanti par l'art. 8, § 1. »

(11) *Van der Velden c/ Pays-Bas*, req. n° 29514/05.

(12) Échantillons qui contiennent beaucoup d'informations sensibles sur un individu et révèlent son code génétique unique.

(13) V. CEDH, *Amann c/ Suisse*, préc., § 69 de l'arrêt.

(14) Informations extraites des échantillons cellulaires, qui se présentent sous la forme d'un code, qui ne peut être déchiffré, et donc utilisé, qu'après une manipulation informatique.

(15) Affaire tranchée par la Commission le 15 mai 1976, req. n° 24950/94.

(16) Arrêt *Kinnunen*, cité par la Cour dans son arrêt *Van der Velden* préc.

(17) V. le II, A.

(18) V. *La Convention européenne des droits de l'homme*, commentaire article par article, sous la direction de L.E. Pettiti, E. Decaux, P.H. Imbert, Économica, 1999, p. 326.

(19) Sunday Times, 26 avr. 1979, req. n° 6538/74, A n° 30, v. GACEDH, p. 434, § 49 : « il faut que la loi soit suffisamment accessible : le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné » et « énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé ». Ces termes sont rappelés pour l'essentiel dans l'arrêt étudié (§ 95).

(20) V. La Convention européenne des droits de l'homme, commentaire article par article, déjà cité, p. 335.

(21) *Rotaru c/ Roumanie*, req. n° 28341//95, arrêt du 4 mai 2000, v. GACEDH, p. 447 ; affaire concernant la détention par le S.R.I. (service roumain de renseignement) de données erronées sur la vie privée du requérant (appartenance prétendue au « mouvement légionnaire roumain », organisation paramilitaire d'extrême droite créée en 1927).

(22) V. O. De Schutter, La Convention européenne des droits de l'homme à l'épreuve de la lutte contre le terrorisme, RUDH 2001. 192.

(23) *Klass c/ République fédérale d'Allemagne*, 6 sept. 1978, série A n° 28, v. GACEDH, p. 432-433.

(24) V. O. De Schutter, La Convention européenne des droits de l'homme à l'épreuve de la lutte contre le terrorisme, RUDH 2001. 191.

(25) *Amann c/ Suisse*, cité ci-dessus, v. note 8. Affaire relative à un homme d'affaires domicilié en Suisse, se plaignant de l'interception d'un appel téléphonique - appel d'une femme depuis l'ambassade soviétique à Berne pour lui commander un appareil dépilatoire - et de l'établissement d'une fiche par le ministère public, dans son fichier destiné à assurer la protection de l'État, ainsi que de la conservation de cette fiche, sans possibilité de recours effectif à cet égard.

(26) À noter cependant que « ce qui avait justifié ici l'applicabilité de l'art. 8 de la Convention, ce n'est pas le simple fait de la conservation de données à caractère personnel, mais plutôt le fait que les données conservées (...) relèvent de la vie privée de l'individu ». V. O. De Schutter, Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel, observations sous l'arrêt *Rotaru*, RTDH 2001.163.

(27) Dans cette affaire, la loi prévoyait simplement la mémorisation par le Service roumain de renseignement et l'utilisation d'informations relatives à la vie privée du requérant, ce qui correspondait au souci de constituer des dossiers secrets de renseignements touchant à la sécurité nationale ; mais aucune disposition du droit interne ne fixait les limites à respecter dans ces prérogatives.

(28) Req. n° 58243/00, 1er juill. 2000. La Cour a noté : « *in conclusion, the Court does not consider that the domestic law at the relevant time indicated with the sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicant's rights under Article 8 was not, therefore, "in accordance with law* ».

(29) V. F. Sudre, *op. cit.*, p. 220.

(30) La Cour fait ici référence à l'art. 9 de la Convention sur la protection des données, dite Convention 108. Art. 9 § 2 :
« il est possible de déroger aux dispositions des art. 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique :
a) à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ».

(31) V. F. Sudre, *op.cit.*, p. 226.

(32) V. par exemple l'arrêt *Klass* du 6 septembre 1978, à propos de la surveillance secrète de la correspondance et des télécommunications des citoyens aux fins de lutte contre le terrorisme : « dans le contexte de l'art. 8, (...) il faut rechercher un équilibre entre l'exercice par l'individu du droit que lui garantit le § 1 et la nécessité, d'après le § 2, d'imposer une surveillance secrète pour protéger la société démocratique dans son ensemble ».

(33) V. La Convention européenne des droits de l'homme, commentaire article par article, déjà cité, p. 341.

(34) CEDH 28 nov. 1984, *Rasmussen c/ Danemark*.

(35) V. F. Sudre, *op. cit.*, p. 229.

(36) CEDH 26 mars 1987, *Leander c/ Suède*, déjà citée.

(37) Sachant que la Convention ne garantit pas en tant que tel le droit d'accès à la fonction publique et que l'ingérence incriminée n'avait pas empêché le requérant de mener sa vie privée à sa guise.

(38) *Z. c/ Finlande*, 25 févr. 1997, req. n° 220009/93 ; affaire particulièrement délicate, concernant une femme contaminée par le VIH, tout comme son époux, contre lequel elle refuse de témoigner au cours de procédures où il était impliqué pour viol et violences sexuelles sur des tierces personnes. La requérante s'est plainte d'une violation de l'art. 8 de la Convention du fait d'ordonnances ayant sommé ses médecins et son psychiatre de témoigner et divulguer des informations la concernant au cours de la procédure pénale dirigée contre son mari, de la saisie de dossiers médicaux et de leur adjonction au dossier d'enquête, des décisions des tribunaux visant à limiter à dix ans la confidentialité du dossier judiciaire et enfin de la divulgation de son identité et de données médicales la concernant dans l'arrêt de la Cour d'Appel.

(39) CEDH 6 juin 2006, définitif 6 sept. 2006, req. n° 62332/80, v. GACEDH, p. 447.

(40) Il n'est pas inintéressant de signaler qu'en France, sont inscrites dans le Fichier Automatisé des Empreintes Digitales (FNAED), les personnes mises en cause dans une procédure pénale ou condamnées à une peine privative de liberté. Quoi qu'il en soit, les empreintes sont conservées vingt-cinq ans. Quant au Fichier National des Empreintes Génétiques (FNAEG), il conserve les empreintes génétiques de personnes condamnées ou simplement mises en cause, pendant quarante ans pour les premières, pendant vingt-cinq ans pour les secondes. Cette longue durée de vingt-cinq ans pour des personnes simplement mises en cause serait-elle jugée conforme à la Convention ? Il est loisible d'en douter...

(41) V. aff. CEDH 21 mars 2000, *Rushiti c/ Autriche*, req. n° 28389/95, § 31. Dans l'affaire 25 août 1993, *Sekanina c/ Autriche*, req. n° 13126/87, la Cour avait noté que « l'on ne saurait s'appuyer à bon droit sur de tels soupçons [sur l'innocence d'un accusé] après un acquittement devenu définitif » (§ 30 de l'arrêt).

(42) C'est nous qui soulignons.

(43) V. § 112 de l'arrêt.

(44) *Ibid.*

(45) *Ibid.*

(46) L'argumentation du Gouvernement britannique est tout à fait révélatrice à cet égard ; il tient en effet à souligner que « la conservation n'aurait pas été motivée par la moindre raison de soupçonner les requérants d'avoir pris part à une infraction ou d'avoir une propension (*sic*) à commettre des infractions ». Cela aurait pu être le cas ?

(47) Comme l'a relevé la Chambre des Lords : v. § 24 de l'arrêt de la Cour.

(48) V. F. Sudre, *Droit européen et international des droits de l'homme*, PUF, 2008, p. 219.

(49) V. Juris-classeur international, La Convention européenne des droits de l'homme, application par les organes de Strasbourg et par les organes nationaux, P. Tavernier, C. Grewe, H. Ruiz Fabri, fasc. 155-E, § 18-19.

(50) *Ibid.* § 53.

(51) V. pour la France par exemple le récent rapport remis par M. Alain Bauer au ministre de l'Intérieur le 11 décembre 2008, « Mieux contrôler la mise en oeuvre des dispositifs pour mieux protéger les libertés », qui fait un état des lieux des fichiers de police et de gendarmerie existants ; la liste est édifiante (fichiers à vocation judiciaire, fichiers de renseignements, fichiers d'antécédents judiciaires, fichiers d'identification judiciaire, systèmes de traitement du renseignement judiciaire...).

(52) V. § 45 de l'arrêt.

(53) *Ibid.*, § 46.

(54) *Ibid.*, § 47. Pour la situation de la France sur ce point, voir ci-dessus note 40.

(55) V. J.-M. Delarue, L'Europe des fichiers - Dialogues des juges, des policiers, des autorités administratives indépendantes *in Le dialogue des juges, Mélanges en l'honneur du Président Bruno Genevois*, Dalloz 2009, p. 279.

(56) On se reportera ici avec profit à l'étude détaillée de J.-M. Delarue citée ci-dessus.

(57) Chaque État est responsable pour sa partie propre du système, le N-SIS, alors que la partie technique commune, le C-SIS, échappe complètement aux États. V. sur ce thème J.-M. Delarue, *op. cit.* p. 278 s.

(58) EUROPOL auquel les services répressifs nationaux ne font que communiquer les données requises.

(59) Comme pour EUROPOL, les autorités nationales se limitent dans EURODAC à alimenter le système central de données.

(60) V. J.-M. Delarue, *op. cit.* p. 279.

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

(62) Avis du 19 déc. 2005, JOUE C 047 du 25/02/2006 ; avis du 29 nov. 2006, JOUE C 091 du 26/04/2007 ; avis du 27 avr. 2007, JOUE C 139 du 23 juin 2007.

(63) V. § 16 et 18 du troisième avis.

(64) V. art. 21 de la Convention EUROPOL par exemple même solution pour EUROJUST, pour la Convention SID, pour le SIS, pour le système issu du traité de Prüm.

(65) Il s'agit d'EUROPOL ici.

(66) V. JOCE L. 281 du 23 nov. 1995, p. 31-50.

(67) À noter que ce texte prévoit en particulier dans son art. 29 la création d'un groupe de travail, appelé « Groupe article 29 » ou « G29 », composé des autorités de contrôle nationales des différents États membres afin de jouer un rôle consultatif auprès de la Commission sur les questions relatives à la protection des données, et de contribuer à une application uniforme des principes généraux des directives dans l'ensemble des États membres.

(68) V. JOCE L 8 du 12 janv. 2001, p. 1-22.

(69) À noter que c'est ce règlement qui a permis la création d'une autorité de contrôle indépendante en la personne du Contrôleur Européen de la Protection des Données ou CEPD, qui dispose de pouvoirs étendus en matière de contrôle du traitement des données à caractère personnel par les organes communautaires, et qui a déjà eu l'occasion de formuler un grand nombre d'avis, extrêmement importants au fond quant à l'argumentation développée, s'agissant en particulier de la proposition de décision-cadre sur la protection des données dans le troisième pilier, mentionnée ci-dessus.

(70) V. JOUE L. 350/60 du 30/12/2008.

(71) Évoquons ici l'affaire *PNR* jugée par la Cour de Justice en 2006 (*Parlement européen c/ Conseil de l'Union européenne et Commission des Communautés européennes, aff. Jtes C-317/04 et C-318/04*). Celle-ci a été amenée à se prononcer sur la légalité, à la fois de la décision 2004/496/CE du Conseil du 17 mai 2004, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure, et de la décision 2004/535/CE de la Commission du 14 mai 2004, relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au bureau des douanes et de la protection des frontières des États-Unis. La décision d'adéquation de la Commission a été annulée au motif qu'elle concerne un traitement de données à caractère personnel exclu du champ d'application de la directive de 1995 par l'article 3 § 2 1er tiret de celle-ci. La décision du Conseil a été également annulée, au motif que l'article 95 du Traité CE et l'article 25 de la directive 95/46/CE (relative à la protection des données, citée ci-dessus) sont insusceptibles de fonder la compétence de la Communauté pour conclure l'accord, car « l'accord vise le même transfert de données que la décision d'adéquation et donc des traitements de données qui sont exclus du champ d'application de la directive » (§ 68 de l'arrêt). Passons sur la pertinence de l'argumentation de la Cour ici (v. par ex. le commentaire de Valérie Michel, *in* RTDE 2006. 535), pour ne retenir que la lacune du droit de l'Union en matière de protection des données que révèle cet arrêt. La décision-cadre « protection des données dans le troisième pilier » est censée combler une telle lacune.

(72) Ce que le CEPD a eu l'occasion de déplorer, comme nous l'avons noté plus haut, car « l'applicabilité de la décision-cadre au traitement national des données est une condition essentielle afin, non seulement d'assurer un niveau de protection suffisant des données à caractère personnel, mais aussi de permettre une collaboration efficace entre les services répressifs ». V. avis du CEPD sur la proposition de décision-cadre, en date du 27 avril 2007, JOUE 23 juin 2007, C 139/1.

(73) V. art. 1 § 4.

(74) V. le troisième avis du CEPD, cité à la note précédente.

(75) Nous pouvons citer simplement trois exemples. Le fait d'abord que le traitement de données dites sensibles, en général prohibées par les autres textes, ne sont ici autorisées « que par une loi » ; on en déduira donc qu'elles sont autorisées... Quant à la durée de conservation des données ensuite, si l'autorité qui transmet les données n'a pas indiqué de délai de conservation, ce sont les délais prévus par le droit national des États membres destinataires qui s'appliquent (art. 9), avec un très grand risque par conséquent de disparité de traitement en la matière. Enfin, quant aux données traitées, il n'est fait aucune distinction entre les différentes catégories de personnes concernées (criminels, suspects, victimes...) ni prévu de garanties spécifiques pour les données relatives aux personnes non suspectes ; cette dernière disposition prend tout son relief dans le contexte de l'arrêt *Marper* de la CEDH étudié ici.

(76) Adopté lors du Conseil européen des 4 et 5 novembre 2004, afin de renforcer l'espace de liberté, sécurité et justice, il a établi un certain nombre de priorités pour la période 2005-2010.

(77) La proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, COM(2005)490 final, est en cours d'adoption.

(78) V. J.-M. Delarue, *op. cit.*, p 276.

(79) V. avis du CEPD sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, 2006/C 116/04, JOUE C 116/8 du 17 mai 2006

(80) V. le point 3.3. de son avis.

(81) V. le point 4.2. de son avis.

(82) V. JOUE C 110/1 du 1er mai 2008.

(83) Il remplace un premier accord conclu en mai 2004, suite à l'annulation par la Cour de Justice de la décision 2004/496/CE du Conseil du 17 mai 2004 dans son important arrêt *Parlement européen c/ Conseil de l'Union européenne et Commission des Communautés européennes*, arrêt *PNR* (v. note 71). Un accord intérimaire avait été conclu le 27 octobre 2006 qui arrivait à échéance le 31 juillet 2007.

(84) Nous sommes en plein dans la problématique de l'affaire *Marper*.

(85) V. § 8 de l'avis.

(86) C'est nous qui soulignons.

(87) V. § 35-36 de l'avis.

(88) V. § 107 de l'arrêt.

(89) V. § 112 de l'arrêt.

(90) Décision-cadre protection des données dans le troisième pilier, 2008/977/JAI citée ci-dessus.

(91) Troisième avis du CEPD sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, en date du 27 avril 2007, JOUE C 139/1 du 23 juin 2007.

(92) C'est nous qui soulignons.

(93) Cet avis a été rendu avant l'arrêt *Marper*... V. le § 20 de l'avis.

(94) V. § 22 de l'avis.

(95) V. le A ci-dessus.

(96) À savoir : les mesures s'appliquent à tous les passagers, qu'ils fassent ou non l'objet d'une enquête des services répressifs ; il s'agit d'investigations proactives, effectuées à une échelle sans précédent. Les décisions relatives aux personnes peuvent se fonder sur des profils abstraits, et comportent donc une marge d'erreur non négligeable. La nature des mesures à prendre à l'encontre de la personne concernée relève de la répression : les conséquences en termes d'exclusion ou de contrainte sont dès lors plus lourdes en termes d'ingérence dans la vie privée que dans un contexte différent, par exemple l'escroquerie à la carte de crédit. V. le § 30 de l'avis.

(97) V. § 31 de l'avis.

(98) V. Henri Labayle, Le juge de l'espace de liberté, sécurité et justice de l'Union européenne, *in Mélanges Genevois*, Dalloz 2009, p. 591 s.

(99) L'article 230 § 4 Traité CE exige en effet que les particuliers soient directement et individuellement concernés par l'acte attaqué, ces conditions ayant été interprétées strictement par la Cour de Justice depuis l'arrêt *Plaumann* (*Plaumann c/ Commission*, 15 juill. 1963, aff. 25/62).

(100) Elle correspond à celle de l'art. 35 § 5 Traité UE actuel. Elle énonce que « dans l'exercice de ses attributions concernant les dispositions des chapitres 4 et 5 du titre V de la troisième partie relatives à l'espace de liberté, de sécurité et de justice, la Cour de justice de l'UE n'est pas compétente pour vérifier la validité ou la proportionnalité d'opérations menées par la police ou d'autres services répressifs dans un État membre, ni pour statuer sur l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure ».

(101) Art. 6 :
« L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007, à Strasbourg, laquelle a la même valeur juridique que les traités ».

(102) Art. 8 :
« 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Les 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 ».

(103) Dans l'arrêt *Parlement européen c/ Conseil* du 27 juin 2006, C-540/03 Rec. CEDH 5769, la Cour avait noté en effet que « s'agissant de la Charte...si cette Charte ne constitue pas un instrument juridique contraignant, le législateur communautaire a cependant entendu en reconnaître l'importance en affirmant, au deuxième considérant de la directive, que cette dernière respecte les principes qui sont reconnus non seulement par l'art. 8 de la CEDH mais également par la Charte ».

(104) Requérant individuel qui pourra former un recours en annulation « contre les actes dont [il] est le destinataire ou qui [le] concernent directement et individuellement, ainsi que contre les actes réglementaires qui [le] concernent directement et qui ne comportent pas de mesures d'exécution » (art. 236, al. 4).

(105) Cour européenne des droits de l'homme, 30 juin 2005, *Bosphorus c/ Irlande*, v. GACEDH p. 741-754, ou v. par ex. le commentaire de Vlad Constantinesco *in* CDE 2006. 363 s.

(106) Une mesure nationale prise en exécution du droit communautaire, nous dit la Cour européenne des droits de l'homme, « doit être réputée justifiée dès lors qu'il est constant que l'organisation en question accorde aux droits fondamentaux (...) une protection à tout le moins équivalente à celle assurée par la Convention. Par 'équivalente', la Cour entend 'comparable' » etc. (§ 155).

(107) V. § 156 de l'arrêt.

(108) V. art. 6 § 2 : « L'Union adhère à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Cette adhésion ne modifie pas les compétences de l'Union telles qu'elles sont définies dans les traités ».

(109) V. Henri Labayle, *op. cit.*, p. 614. L'auteur ajoute : « l'éventualité de cette adhésion et de l'admission du contrôle de la Cour européenne ne change rien à l'urgence qu'il y a à approfondir son action de régulation et de contrôle ».

(110) V. CJCE 20 mai 2003, *Österreichische Rundfunk*, aff. jointes C-465/00, C-138/01, C-139/01.