Cultures & Conflits

76 (hiver 2009)
Fichage et listing

Rocco Bellanova et Paul De Hert

Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen

Référence électronique
Rocco Bellanova et Paul De Hert, « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011, consulté le 01 janvier 2013. URL : http://conflits.revues.org/17805

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

Document accessible en ligne sur : http://conflits.revues.org/17805
Ce document est le fac-similé de l'édition papier.

Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen *

Rocco BELLANOVA, Paul DE HERT

Rocco Bellanova fait partie du Centre de recherche en science politique *aux* Facultés universitaires Saint-Louis *et du centre de recherche* Law, Science, Technology & Society *à la* Vrije Universiteit Brussel.

Paul De Hert fait partie du centre de recherches Law, Science, Technology & Society *à la* Vrije Universiteit Brussel *et du* Tilburg Institute for Law and Technology *à la* Tilburg University.

Lu roggiu di lu Sant'Ufficiu nun cunzigna mai [1].

De plus en plus, les systèmes de sécurité font appel à des technologies de l'information visant à collecter, conserver et traiter des données personnelles. Même si la surveillance, la gestion et le contrôle des individus et des populations s'ancrent dans une histoire longue [2], l'introduction de ces nouvelles technologies semble contribuer à modifier l'objectif que leur assigne les pouvoirs publics, le réorientant vers la prévention et le contrôle « à distance » des possibles menaces ou crimes [3]. Les données ne sont plus seulement collectées et stockées à des fins de procédure judiciaire, mais elles sont accumulées et thésaurisées, pour agir « le cas échéant » [4].

---

* . Les auteurs remercient vivement Pierre Piazza pour ses commentaires et son patient travail de révision linguistique.

1 . « L'horloge du Saint Office ne libère jamais », Sciascia L., *Morte dell'inquisitore*, Milano, Adelphi, 1992, p. 22.

2 . Le recours aux données personnelles par la police n'est pas une nouveauté, il suffit de penser au développement du « bertillonnage » en France ou à l'introduction des empreintes digitales dans les colonies britanniques au XIXe siècle. Cf. notamment Piazza P., « Alphonse Bertillon face à la dactyloscopie. Nouvelle technologie policière d'identification et trajectoire bureaucratique », *Les Cahiers de la sécurité intérieure*, nº 56, 2005, pp. 251-270 ; Cole S. A., *Suspect identities: A History of Fingerprintings and Criminal Identification*, Cambridge (Massachussetts), Harvard University Press, 2002.

De plus, ces technologies de contrôle sont souvent définies comme « smart », pour signifier que l'on recourt à des systèmes informatiques ayant un haut degré d'automatisation. Elles sont aussi définies comme « *soft* », pour indiquer qu'elles occasionnent de moindres conséquences négatives sur la vie individuelle et sociale [5]. La collecte, la conservation et le traitement des données biométriques, comme les empreintes digitales, la captation de l'iris réalisée à l'aide d'une caméra et les échantillons d'ADN, paraissent réunir toutes ces caractéristiques. D'une part, ces mesures sont présentées comme « soft » : la collecte serait rapide, pourrait se passer de la coercition et serait même opérée sur une base volontaire [6]. De plus, la conservation n'aurait de conséquences négatives sur les individus que lorsque qu'ils ont commis une infraction et, au contraire, aurait un impact positif permettant de réduire les cas d'inculpation erronée et d'innocenter rapidement un bon nombre de suspects [7]. D'autre part, ces mesures seraient aussi « *smart* » : une large base de données constituerait un atout fondamental. Traitée par des logiciels particulièrement performants, ce type de base deviendrait capable de réduire le temps d'investigation et d'améliorer l'efficacité de la police. De surcroît, elle permettrait de guider les ressources humaines sur les suspects les plus probables, en dressant des profils de criminels et offrirait aussi des solutions aux cas que l'on n'aurait pas pu résoudre précédemment [8]. Donc, étant donné le caractère peu intrusif et presque invisible de chaque partie du système, ce contrôle diffus ne pourrait, selon certains, engendrer aucune véritable atteinte à la vie privée.

Dans un tel contexte, le 8 décembre 2008, la Cour européenne des droits de l'homme (CEDH) a prononcé un arrêt décisif en matière de protection de la vie privée (telle que définie par l'article 8 de la Convention européenne des droits de l'homme) [9]. M. S. et M. Marper, deux citoyens du Royaume-Uni

3 . Guid E. et Bigo D., « Le visa Schengen : expression d'une stratégie de «police» à distance », *Cultures & Conflits*, n° 49, 1/2003 pp. 22-37.

4 . On remercie Julien Jeandesboz pour nous avoir conseillé cette image du « cas échéant ».

5 . Marx G.T., « Soft Surveillance. The Growth of Mandatory Volunteerism in Collecting Personal Infomation - "Hey Buddy Can You Spare a DNA?" », *in* Monahan T. (ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*. New York/London, Routledge, 2006, pp. 37-56.

6 . *Ibid.*

7 . Etzioni A., « DNA Tests and Databases in Criminal Justice: Individual Rights and the Common Good », *in* Lazer D. (ed.), *DNA and the Criminal Justice System: The Technology of Justice*. Boston, MIT Press, 2004, pp. 197-223.

8 . *Ibid.*

9 . CEDH, *S. et Marper c. Royaume Uni*, *Requêtes nos 30562/04 et 30566/04*, Strasbourg, 4 décembre 2008. Dorénavant dans cet article, cet arrêt sera cité comme « *Marper* » et il sera fait, par la suite, référence à ses paragraphes. L'article 8 « Droit au respect de la vie privée et familiale » stipule : « 1) Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2) Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que 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 ».

avaient saisi la CEDH pour se plaindre de la conservation de leurs empreintes digitales, de leurs profils et échantillons d'ADN dans les banques de données de la police britannique, alors même qu'ils avaient été mis hors de cause ou acquittés [10]. L'effacement de ces données leur avait préalablement été refusé par les autorités de police, ainsi que par tous les autres niveaux juridictionnels, sur la base du *Police and Criminal Evidence Act* (une loi de 1984 relative à la police et aux preuves en matière pénale [11]). L'arrêt de la CEDH est une victoire pour la vie privée parce que la conservation pour une durée illimitée des empreintes digitales, des échantillons cellulaires et des profils ADN des personnes non condamnées est reconnue comme une violation de l'article 8 de la Convention européenne des droits de l'homme [12]. Compte tenu du système technologique mobilisé et des pratiques policières dont il est question, l'arrêt devient encore plus important car il fixe des limites à la « simple conservation » des données privées et en souligne le caractère stigmatisant.

Le cas de S. et Marper

Les faits

Lors de leur arrestation en 2001, les empreintes digitales des deux requérants, S. et Marper, avaient été relevées et leurs échantillons d'ADN prélevés [13]. S. était alors mineur et il a ensuite été acquitté quelques mois plus tard. Quant à Marper, il a vu son affaire être classée sans suite [14]. Tous deux demandèrent par la suite la destruction de leurs empreintes et échantillons d'ADN qui ne fut pas acceptée par la police [15]. Un refus leur fut également opposé par le Tribunal administratif, la Cour d'appel et la Chambre des Lords [16]. Les requérants estimaient non seulement que la conservation de leurs données était une ingérence dans leur droit à la vie privée, mais aussi qu'elle « faisait peser des soupçons sur des personnes ayant bénéficié d'un acquittement » [17].

10 . Les requérants ont saisi la CEDH non seulement sous l'angle de l'article 8 de la Convention européenne des droits de l'homme, mais aussi sous l'angle de l'article 14 (« Interdiction de discrimination »), *Marper*, §3. Cependant, la CEDH ne se prononce pas sur le grief concernant ce dernier article, cf. *Marper*, §129.

11 . Cf. *Marper*, §§26-29. Cette loi permet la conservation pour une durée illimitée des données biométriques collectées lors de l'arrestation, même lorsque les individus sont mis hors de cause ou acquittés.

12 . Cf. Marper, §§105-126. Pour synthétiser : « 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 », *Marper*, §125.

13 . S. avait été inculpé de tentative de vol avec violence et Marper de harcèlement à l'égard de sa compagne. *Marper*, §§10-11.

14 . *Ibid.*

15 . *Marper*, §12.

16 . *Marper*, §§12, 13 et 15.

17 . *Marper*, §21.

Devant la CEDH, ils ont contesté la justification de cette mesure par rapport aux critères définis par le second paragraphe de l'article 8 de la Convention européenne des droits de l'homme. Les objectifs du traitement des données seraient « vagues et se prêteraient à des abus ». De plus, les garanties procédurales contre les usages impropres ou abusifs de ces informations seraient insuffisantes [18]. Enfin, la conservation pendant une durée illimitée de données biométriques de personnes non condamnées ne peut passer pour « nécessaire dans une société démocratique », compte tenu que cette conservation un caractère disproportionné et « jetterait le doute sur des personnes ayant été acquittées ou ayant bénéficié d'un non-lieu, car cela laisserait entendre qu'elles n'étaient pas totalement innocentes » [19].

Même si le gouvernement britannique a accepté que les données biométriques collectées soient qualifiées de données personnelles, il prétendait que leur conservation « ne porterait pas atteinte à l'intégrité physique et psychologique de la personne et ne méconnaîtrait pas non plus le droit à l'épanouissement personnel, le droit de nouer et développer des relations avec ses semblables ni le droit à l'autodétermination » [20]. Il a aussi soutenu que « l'ingérence serait nécessaire et proportionnée aux buts légitimes que constituent la défense de l'ordre et la prévention des infractions pénales et/ou la protection des droits et libertés d'autrui », et que le matériel conservé représentait « une valeur inestimable aux fins de la lutte contre la criminalité et le terrorisme » [21]. Finalement, le gouvernement britannique a refusé d'établir un lien entre conservation des données et stigmatisation puisque « 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 à commettre des infractions (…) [mais] parce que la police les avait déjà légalement en sa possession et parce qu'elles pouvaient contribuer à l'avenir à la prévention et à la détection des infractions en général grâce à l'élargissement de la base de données » [22].

Les principales conclusions de la CEDH

L'article 8 de la Convention européenne des droits de l'homme protège la vie privée, mais il n'intègre pas automatiquement la protection des données personnelles [23]. Traditionnellement, pour la CEDH, toutes les données personnelles ne jouissent pas de la protection de la vie privée. Elle opère donc une

18 . *Marper*, §87.

19 . *Marper*, §§88-89. Par ailleurs, une limitation de l'article 8(1) de la Convention peut être justifié seulement si les trois critères définis à l'article 8(2) sont remplis cumulativement : la limitation doit être prévue par la loi ; et elle doit poursuivre un but légitime ; et elle doit être nécessaire dans une société démocratique.

20 . *Marper*, §63.

21 . *Marper*, §90. En appui à ses thèses, le gouvernement cite les statistiques et les résultats liés à la conservation (et au traitement) des données des individus non coupables, cf. *Marper*, §§91-93.

22 . *Marper*, §94.

analyse au cas par cas de la nature, du traitement et du contexte de la collecte des données, pour établir leur pertinence aux sens de l'article 8 de la Convention européenne des droits de l'homme. Dans le cas S. et Marper, la CEDH estime que les trois types de données qui font l'objet du cas examiné sont à considérer comme des données « privées » [24]. Même si la Cour opère une distinction entre les trois types de données (échantillons et profils ADN et empreintes digitales) et qu'elle justifie la pertinence de l'application de l'article 8 de manière différenciée pour chacune d'entre elles, il y a là une avancée significative : la conception des données dignes de protection est, de facto, élargie de manière significative.

Le deuxième élément fondamental de l'arrêt S. et Marper est le choix explicite opéré par la CEDH de s'intéresser au critère de la « nécessité dans une société démocratique » [25]. Auparavant, elle avait souvent évité de focaliser son analyse sur cet aspect et portait davantage son contrôle sur d'autres critères plus « techniques », comme par exemple la condition de légalité. Dans le cas étudié, la CEDH rompt avec une telle logique et, après une longue analyse des principes et du droit comparé [26], elle conclut à l'illégitimité et au caractère disproportionné des bases de données dactyloscopique et génétique instituées au Royaume-Uni [27].

---

23 . Il y a là une différence majeure avec la Charte des droits fondamentaux de l'Union européenne qui a constitutionnalisé à la fois la protection de la vie privée (art. 7) et la protection des données personnelles (art. 8).

24 . De Beer D., De Hert P., Gonzalez Fuster G. et Gutwirth S., « Nouveaux éclairages de la notion de "donnée personnelle" et application audacieuse du critère de proportionnalité », Cour européenne des droits de l'homme, Grande Chambre *S et Marper c. Royaume Uni*, 4 décembre 2008, *Revue Trimestrielle des Droits de l'Homme*, nº 81, 2010, pp. 144-154.

25 . De Beer et *al.*, *op.cit.*, p. 155-159.

26 . « 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 », *Marper*, §101. L'analyse de droit comparé se fait dans §§45-55, et, plus loin, la Cour conclut 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. […] 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 », *Marper*, §112. Par contre, comme observé ailleurs, le recours au droit comparé n'est pas sans danger, cf. De Beer et *al.*, *op.cit.*, p. 159.

27 . En effet, elle 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 », *Marper*, §125.

Un troisième élément d'importance dans l'arrêt a trait à la position de la CEDH en ce qui concerne l'acte de la « simple » conservation des données privées. Existe-t-il un danger au regard de la vie privée quand l'acteur responsable d'une base de données ne fait rien avec les informations qu'elle contient ? Pour mieux apprécier la position de la CEDH, que l'on ose qualifier de révolutionnaire, il faut remonter un peu dans le temps et s'arrêter sur un jugement antérieur : le cas Friedl [28].

La stigmatisation liée au traitement et à la conservation des données personnelles

Flash-back : le cas Friedl

L'affaire Friedl contre l'Autriche concerne l'utilisation de photographies et de données d'identité de M. Friedl, rassemblées par la police à l'occasion d'une manifestation. Le 12 février 1988, Friedl organisait, avec d'autres individus, un sit-in dans une station de métro à Vienne dans le but de mener une action en faveur des sans-abri. Selon les faits tels qu'ils sont repris dans l'arrêt, différents usagers du métro auraient introduit des plaintes auprès des autorités à propos des perturbations occasionnées par les participants à cette manifestation. Le 19 février 1988, la police pria les personnes impliquées de mettre fin à leur initiative, et leur fit savoir que l'absence d'autorisation pour la manifestation constituait une violation de l'article 82 de la *Straßenverkehrsordnung* [29]. Les participants n'obtempérèrent pas immédiatement à cette injonction, ce qui motiva le déclenchement par les forces de l'ordre d'une opération de contrôles d'identité sur 57 personnes et de prise de photographies et d'images vidéo.

Friedl saisit la Cour Constitutionnelle autrichienne le 21 mars 1988. A ses yeux, le fait qu'on ait relevé son identité, pris des photographies de sa personne et interrompu le sit-in constituait autant de violations flagrantes de l'article 8 (droit au respect de la vie privée) et de l'article 11 (droit au rassemblement pacifique) de la Convention européenne des droits de l'homme. Le gouvernement soutint que l'intention des services de police n'était nullement d'identifier les participants individuellement. Les données personnelles et les images collectées ne furent aucunement introduites dans une banque de données. Les photographies et les dossiers administratifs élaborés à propos du sit-

28 . CEDH , *Friedl c/ Autriche*, 31 janvier 1995, Série A. vol 305-B. Commission européenne des droits de l'homme, *Friedl c/ Autriche*, 19 mai 1994, *requête n° 15225/89*. A présent, dans notre article, cet arrêt sera cité ainsi « *avis Friedl* ».

29 . L'article 82 du code de la route autrichien, *Straßenverkehrsordnung*, sanctionne toute entrave à la circulation des piétons, *arrêt Friedl*, §7.

30 . Jusqu'à 1998, la Convention prévoyait deux organes : la Commission des droits de l'homme et la Cour des droits de l'homme. La Commission était compétente sur la recevabilité des requêtes et établissait des « rapports » sur les cas déclarés recevables, et la Cour pouvait réexaminer les affaires et rendre des arrêts.

in seraient détruits en l'an 2001, c'est-à-dire dix ans après leur dernière consultation par la police. La Cour autrichienne rejeta les plaintes de Friedl le 13 décembre 1988. Sur la prise de photographies et le traitement de données personnelles, elle déclara ne pouvoir exercer aucun contrôle étant donné que ses compétences ne portent que sur des contrôles d'ordre administratif et sur le recours à des violences physiques.

Le 5 juin 1989, Friedl se tourna vers la Commission des droits de l'homme de Strasbourg [30]. Là, il répéta ses arguments concernant l'atteinte aux articles 8 et 11 de la Convention européenne des droits de l'homme, auxquels il en ajouta un autre portant sur une violation de son droit à pouvoir saisir une quelconque instance juridictionnelle pour contester les pratiques qu'il avait eu à subir (à laquelle il avait droit au regard de l'article 13 Convention européenne des droits de l'homme lorsqu'un droit du Traité est violé). Plus spécifiquement à propos de l'article 8, il allégua que la police de Vienne n'avait, en l'occurrence, aucun besoin de traiter des données personnelles dans un cas relevant de la police administrative, d'autant qu'il n'y avait aucune intention de poursuite.

Dans son rapport, la Commission des droits de l'homme déclara seules recevables les plaintes se rattachant aux articles 8 et 13, mais elle estima qu'il n'y avait aucune violation de ces articles pour ce qui concerne la prise et la saisie d'images [31]. Elle précisa cependant que le fait de relever et de rassembler des données personnelles au cours de la manifestation (compte tenu du manque de possibilité pour le requérant de déposer plainte devant une Cour à propos de cette pratique [32]) violait l'article 13. L'avis de la Commission des droits de l'homme sur Friedl est particulièrement important. En effet, à cette occasion, elle a estimé que le stockage de données par la police peut être considéré comme une nécessité dans une société démocratique, compte tenu que ces données sont simplement conservées dans un dossier administratif et qu'elles ne sont aucunement saisies dans une banque de données [33]. Donc, parce qu'il n'y a pas d'exploitation ou d'« usage critique » de ces données, il ne saurait y avoir de problème de vie privée.

---

31 . En ce qui concerne l'article 8 : cf. *avis Friedl*, §§52 et 68l. Cf. aussi *avis Friedl*, §73 pour l'article 13.

32 . *Avis Friedl*, §80. L'affaire fut renvoyée devant la Cour, mais celle-ci ne prononça pas de jugement sur le fond de l'affaire. En effet, par missive du 22 décembre 1994, la Cour apprit du représentant du gouvernement autrichien que le gouvernement et Friedl étaient arrivés à une conciliation. Friedl fut dédommagé financièrement pour le préjudice subi, et toutes les photographies et leurs négatifs furent détruits. On demanda alors à la Cour de rayer l'affaire du rôle. Cf. *arrêt Friedl*, §§15-17.

33 . Il faut souligner qu'en ce qui concerne la prise des photos et leur conservation, la Commission ne considéra pas ces pratiques comme une « ingérence dans [le] droit [du requérant] au respect de sa vie privée, aux termes de l'article 8 § 1 de la Convention », §53, *avis Friedl*. Quant à la conservation des information sur l'identité, la Commission rappelle que la « conservation des dossiers relatifs à des affaire pénales antérieures est considérée comme nécessaire, dans une société démocratique, à la prévention de la criminalité et que, quand bien même aucune procédure ne serait subséquemment engagée et qu'aucun soupçon raisonnable

Cette position adoptée par la Commission des droits de l'homme sur la « simple » conservation des données personnelles apportait peu de réponses juridiques au développement des pratiques de « soft » surveillance [34]. L'individu était finalement découragé d'agir et se devait de « supporter » le fait d'être enregistré dans des bases de données policières. Un possible recours ne s'offrait à lui qu'à partir du moment où quelque chose se produisait quant à l'utilisation de ses données, par exemple quand la police y recourait d'une manière telle que des conséquences négatives pouvaient se produire pour sa personne. Comment dès lors, dans ce contexte, limiter la conservation dans les fichiers de la police de données personnelles d'individus non suspects et non poursuivis ?

La nouvelle approche de la CEDH : un « exit » de l'impasse

La posture de la CEDH dans le cas S. et Marper semble plus tranchée par rapport à l'enjeu de la conservation des données. Dans son approche, trois « moments » apparaissent importants. Le premier est relatif à l'analyse préalable de la pertinence des données personnelles au sens de l'article 8. Une fois que l'on considère que les données personnelles concernent la vie privée d'un individu (et on a déjà vu le progressif élargissement de cette conception), un « second moment » consiste à se référer à la jurisprudence liée à l'arrêt Leander qui porte sur la mémorisation des données relatives à la vie privée dans un registre secret de la police [35]. Dans ce cas, la CEDH avait conclu que cette pratique policière n'était pas contraire à l'article 8 car elle était justifiée au regard des trois critères établis par le paragraphe 2 de l'article 8. Néanmoins, la CEDH avait alors reconnu que le simple fait de mémoriser ces données constituait une ingérence [36]. Enfin, « troisième moment », la CEDH précise : « peu importe que les informations mémorisées soient ou non utilisées par la suite » [37]. Ainsi, l'important ici en matière de protection de données est que, finalement, la CEDH sort de l'impasse de la « simple » conservation

ne pèserait sur l'individu quant à une infraction spécifique, des conditions particulières telles que le combat contre le terrorisme organisé, peuvent justifier la conservation des documents incriminés. (…) Les informations obtenues furent conservées dans un dossier administratif général consignant les événements. Elles ne furent, en outre, saisies dans aucun système de traitement de données. La Commission constate dès lors, en prenant en considération la marge d'appréciation accordée en ce domaine aux Etats contractants, que l'ingérence relativement légère dans le droit du requérant au respect de sa vie privée peut raisonnablement passer pour nécessaire, dans une société démocratique, à la défense de l'ordre et à la prévention des infractions pénales », *avis Friedl*, §67.

34. De Hert P. « Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11 », *Utrecht Law Review*, Vol.1(1), 2005, pp. 68-96.

35 . CEDH, *Leander c/ Suede*, *requête no 9248/81*, Strasbourg, 26 mars 1987.

36 . *Ibid.*, §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'article 8 paragraphe 1 ».

37 . *Ibid.*, faisant cette fois référence à l'affaire Amann : CEDH, *Amann c/ Suisse*, *requête n° 27798/95*, Strasbourg, 16 février 2000.

et remet en cause l'idée selon laquelle le stockage dans les bases de données de la police est un acte que l'on peut considérer comme « neutre ». Dans ses conclusions, elle réaffirme d'ailleurs que « le simple fait de la conservation ou de la mémorisation de données à caractère personnel par les autorités publiques (…) 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 » [38].

La présomption d'innocence : inapplicable dans le cadre de la surveillance « douce »…

Une source de perplexité dans la pratique des droits de l'homme est l'étendue plutôt restreinte du principe de la présomption d'innocence et le droit de ne pas s'incriminer soi-même (*nemo tenetur*). Ces principes, pourtant souvent évoqués par les militants anti-surveillance à l'encontre de la généralisation des techniques d'espionnage, ne resurgissent que rarement dans les débats juridiques consacrés à ce sujet. Le principe de la « présomption d'innocence » est défini par l'article 6 (paragraphe 2) de la Convention européenne des droits de l'homme selon lequel : « Toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie » [39]. Or, le principe de la « présomption d'innocence » est un droit procédural et il est, comme tel, soumis à certaines limites. En tant que droit de la défense, il ne couvre que les personnes « accusées d'une infraction », et cette infraction doit être de nature pénale [40]. C'est la raison pour laquelle ce droit ne peut pas toujours être invoqué [41]. Par contre, on peut affirmer que parmi les objectifs de ce

38 . *Marper*, §121. Il est vrai que, d'une certaine manière, les considérations sur le (possible) traitement des données restent encore fondamentales pour la décision concernant leur caractère « privé », et donc il y a encore possibilité de divergence entre ce qui pourrait être protégé par l'article 8 de la Convention européenne des droits de l'homme et la protection de données. Par contre, les derniers jugements paraissent confirmer une tendance vers une compréhension accrue de la CEDH des enjeux et mécanismes de la protection de données. Cf. notamment CEDH, Bouchacourt c. France (*requête no 5335/06*), Strasbourg, 17 décembre 2009, §57 : « la Cour relève que le FIJAIS [fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes] contient des données relatives à la vie privée du requérant. […] La Cour souligne qu'il ne lui appartient pas de spéculer sur le caractère sensible ou non des éléments recueillis ni sur les éventuels inconvénients subis par le requérant. Selon sa jurisprudence, la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu » ; et §61 « La protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. […] A l'instar de ce qu'elle a décidé dans l'arrêt *S. et Marper c. Royaume-Uni* […] la Cour est d'avis que 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 ».

39 . Le même principe est aussi établi par l'article 48 de la Charte des droits fondamentaux de l'Union européenne qui précise : « Tout accusé est présumé innocent jusqu'à ce que sa culpabilité ait été légalement établie ».

40 . « La présomption d'innocence ne bénéficie qu'aux personnes accusées d'une infraction pénale au sens de la Convention, c'est-à-dire aux "personnes inculpées, prévenues ou accusées d'une infraction pénale" », Kuty F. (2006). *Justice pénale et procès équitable*. Vol. 2. Bruxelles, Larcier, p. 206.

droit il y a celui de définir les catégories de « coupable » et « innocent », et de limiter l'étendue de la catégorie de « suspect ». En effet, si la catégorie de « suspect » est, *per se*, liminale, et donc transitoire, elle reste aussi subordonnée à celle d'« innocent » grâce à la présomption d'innocence, qui garantit durant la période pendant laquelle l'individu est considéré comme innocent toutes une série de droits à la défense.

La Convention européenne de sauvegarde des droits de l'homme ne mentionne aucun droit fondamental au silence. Dans l'arrêt Funke de 1993, la CEDH affirme néanmoins que le principe *nemo tenetur* est protégé par la Convention européenne de sauvegarde des droits de l'homme [42]. Et dans l'arrêt Murray datant de 1996, elle ajoute que le droit de se taire pendant un interrogatoire de police et le droit de ne pas contribuer à sa propre incrimination sont des normes internationales généralement reconnues qui sont au coeur de la notion de « procès équitable » (au sens de l'article 6 de la Convention européenne de sauvegarde des droits de l'homme), même s'ils ne sont pas spécifiquement mentionnés par cet article. En mettant le prévenu à l'abri d'une coercition abusive de la part des autorités, ces immunités concourent à éviter des erreurs judiciaires et à garantir l'objectif que vise l'article 6 [43]. L'arrêt Murray s'avère donc être d'une grande importance pour la police parce que la CEDH se prononce sur la question de savoir si le fait qu'un prévenu se taise pendant un interrogatoire de police peut par la suite être utilisé contre lui.

Plusieurs auteurs et autorités de protection des données se sont penchés sur la question de savoir si l'article 6(2) pouvait aussi s'appliquer pour des systèmes collectant, conservant et exploitant des données personnelles [44]. Collecter et conserver « par défaut » les données personnelles d'un grand nombre de personnes paraît non seulement toucher à leur vie privée, mais aussi à la signification et à la validité de la catégorie « innocent ». Ni coupable,

41. « Le champ d'application de l'article 6, § 2 de la Convention ne se limite toutefois pas aux procédures pénales pendantes. Il s'étend encore aux personnes qui ont fait l'objet d'une décision de justice, notamment de nature civile, prise après l'arrêt des poursuites. La garantie de l'article 6, § 2 (…) s'étend dès lors aux procédures judiciaires postérieures à l'acquittement définitif du prévenu », Kuty F., *ibid.*, p. 207.

42 . CEDH, *Jean-Gustave Funke c/ France*, Strasbourg, 25 février 1993, §44 ; N.J., 1993, n° 485, note Kn. ; J.D.F., 1993, n° 1-2, note M.B. On lira au sujet de cet arrêt : Swart A., « Bewijs leveren tegen zichzelf », *Ars Aequi*, 1993, pp. 672-680 ; Myjer E., « Zwijgen op aangeven van de douane », *NJCM*, 1993, n° 5, pp. 584-592 ; Yernault D., « Les pouvoirs d'investigation de l'administration face à la délinquance économique : les locaux professionnels et l'article 8 de la Convention européenne », note sous *Miailhe c. France*, *R.T.D.H.*, 1994, p. 121.

43 . CEDH, *John Murray c/ Royaume-Uni*, Strasbourg, 8 février 1996, §45.

44 . De Hert P., *op.cit.*, pp. 84-86 ; Steinbock D.J., « Data Matching, Data Mining, and Due Process », *Georgia Law Review*, Vol. 40(1), 2005, pp. 1-86 ; Koops E.J., Prinsen M.M., « Houses of glass, transparent bodies: How new technologies affect inviolability of the home and bodily integrity in the Dutch constitution », *Information & Communications Technology Law*, Vol. 16(3), 2007, pp. 177-190. Cf. aussi: European Data Protection Supervisor (2008). *Preliminary Comments of the European Data Protection Supervisor on: - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, « Preparing the next steps in border management in the European Union », COM(2008) 69 final*; Bruxelles, EDPS, pp. 5-6.

ni innocent, un nombre grandissant d'individus se retrouveraient « suspects », c'est-à-dire stigmatisés par rapport à leur statut officiel d'innocent, mais sans avoir à subir les mêmes conséquences que les personnes considérées comme coupables.

En droit, pourtant, le principe de la présomption d'innocence et le droit de ne pas s'incriminer soi-même ne constituent aucunement une protection contre l'utilisation des technologies douces ou « *smart* ». Dans l'arrêt Saunders c. le Royaume-Uni [45], la CEDH donne une interprétation restrictive du principe *nemo tenetur*, en l'assimilant au droit au silence : le principe *nemo tenetur* de l'article 6 de la Convention européenne de sauvegarde des droits de l'homme ne se rapporte qu'au droit de ne pas faire de déclarations. Elle explique ce point de manière très détaillée dans l'important paragraphe 69 : « Le droit de ne pas s'incriminer soi-même concerne en premier lieu le respect de la détermination d'un accusé de garder le silence. Tel qu'il s'entend communément dans les systèmes juridiques des parties contractantes à la Convention », et, poursuit la CEDH, ce droit « ne s'étend pas à l'usage, dans une procédure pénale, de données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté du suspect, par exemple, les documents recueillis en vertu d'un mandat, les prélèvements d'haleine, de sang et d'urine ainsi que de tissus corporels en vue d'une analyse de l'ADN » [46].

…ou bien nouveau garde-fou ?

Ce qui précède explique l'importance du droit à la protection de la vie privée pour ce qui concerne la surveillance. Les droits de la défense contenus dans l'article 6 de la Convention européenne de sauvegarde des droits de l'homme sont inefficients dans le cadre de la problématique de la surveillance contemporaine. L'affaire Marper est remarquable parce qu'elle semble mettre fin à cette situation. En effet, dans cette affaire, la CEDH fait référence à la présomption d'innocence et elle l'articule dans sa réflexion avec les enjeux de la stigmatisation et de la conservation des données dans un même paragraphe (le §122). Ce paragraphe mérite une attention toute particulière. On peut y lire : « 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 » [47].

45 . CEDH, *Saunders c/ Royaume-Uni*, Strasbourg, 17 décembre 1996.
46 . *Ibid.*, §69.
47 . *Marper*, §122.

Pour mieux comprendre la démarche de la CEDH, il faut d'abord rappeler qu'elle refuse d'analyser le grief des requérants sous l'angle de l'article 14 de la Convention européenne de sauvegarde des droits de l'homme relatif à la discrimination. En outre, la CEDH ne se penche pas directement sur l'article 6(2), parce qu'il n'a pas été invoqué et ne pourrait, fort probablement, pas être appliqué. Elle paraît plutôt s'ingénier à discuter les risques de stigmatisation des mesures en question, à définir leur nature et à préconiser certains garde-fous. Elle semble identifier la stigmatisation comme le risque de pérennisation de la catégorie de « suspect » qui prend forme à travers la pratique consistant à procéder à la même conservation des données privées relatives aux criminels et aux personnes innocentes. La référence au cas Rushiti contre Autriche [48], qui vient à la suite du paragraphe 122 cité précédemment, semble supporter l'argumentaire du lien que l'on peut établir entre la nature des pratiques de surveillance et l'expression de soupçons. Dans ce cas, la CEDH avait affirmé qu'on ne peut plus, à propos d'une affaire, exprimer de soupçons à l'encontre de quiconque a été mis hors de cause consécutivement à une accusation [49].

Dans le cas S. et Marper, la CEDH vise à limiter la pérennisation de la confusion susceptible d'être établie entre personnes innocentes et accusées en développant une argumentation en trois étapes. Tout d'abord, elle estime que, eu égard à la portée et à la spécificité du traitement des données en question, leur conservation devient une atteinte à la vie privée et ne saurait être considérée comme banale. La CEDH aborde ensuite l'enjeu de la temporalité de la conservation des données qu'elle relie implicitement à celui de la proportionnalité de la mesure : mobiliser la même temporalité de conservation des données, et donc la même proportionnalité, pour les suspects (ou anciens suspects) et les criminels, engendrerait une « fracture » au sein de la catégorie des « innocents ». En effet, parce qu'elle n'est pas anodine, la conservation sanctionnerait de manière disproportionnée une partie des individus relevant de la catégorie des innocents en les reliant au statut de criminel. C'est pourquoi, la CEDH considère enfin qu'il est possible d'apporter une réponse à ce problème et à la stigmatisation qui en découle en imposant des limites temporelles à la conservation des données pour les personnes innocentes.

Cette articulation du raisonnement autour de la présomption d'innocence et sur son effet désiré est tout à fait intéressante ici, même si elle s'opère en grande partie de manière cachée en s'appuyant sur l'argument de la protection de la vie privée, et plus particulièrement sur celui de l'importance de la « simple » conservation des données privées. La stigmatisation semble donc enfin trouver une réponse juridique, ne serait-ce que d'une façon indirecte.

48 . CEDH, *Rushiti c/ Autriche*, *requête no 28389/95*, Strasbourg, 21 mars 2000.
49 . *Ibid.*, §31.

L'horloge de la stigmatisation stoppée

L'attention accordée à la dimension temporelle de la conservation nous fait penser aux caractéristiques de l'horloge du proverbe sicilien cité en exergue. L'horloge du Saint Office ne sonne jamais l'heure de la libération d'un individu : dès qu'on entre dans le système, c'est à jamais. Par contre, l'horloge de l'état de droit sonne toujours, et elle annonce soit la culpabilité soit la libération. Dans le cas S. et Marper, la CEDH insiste sur les incidences de la conservation des données, ce qui pourrait être assimilable au mouvement de l'horloge, mais elle vise aussi à établir des limites temporelles pour éviter les discriminations (des alarmes qui font sonner l'horloge et permettent de libérer les individus). Elle souligne donc que la conservation des données personnelles pour une durée indéfinie (au moins pour les innocents) équivaut à rendre l'horloge légale silencieuse et à la placer hors des cadres d'une société démocratique. L'arrêt étudié met en évidence l'impact des mesures et des technologies de sécurité sur la vie privée, même quand elles paraissent opérer en « *stand-by* » comme dans le cas d'une « simple » conservation des données. À travers le raisonnement développé sur la conservation et la stigmatisation, la CEDH non seulement se démontre plus attentive à la protection des données, mais elle paraît aussi identifier dans sa démarche une possibilité de limiter les effets de la surveillance, aussi « *soft* » ou « *smart* » soit-elle.