UNIVERSITE MONTPELLIER I

FACULTÉ DE DROIT
UNITÉ DE FORMATION ET DE RECHERCHE

LICENCE 3
2016-2017, premier semestre

Equipe pédagogique
Pierre-Yves GAHDOUN, Professeur
Mathilde KAMAL, Chargée de travaux dirigés
Yannick RAJAONSON, Chargé de travaux dirigés

Droit des libertés fondamentales

-TRAVAUX DIRIGÉS-

SÉANCE 5

Données personnelles et libertés fondamentales

DOCUMENTS :

I – Cadre juridique

1. Loi n°78-17 du 6 janvier 1978 dite « informatique et libertés »
2. CC, décision n°2012-652 DC du 22 mars 2012

II – Applications
A – La protection des atteintes commises par les personnes privées

3. C. RICHAUD, « Données personnelles : la schizophrénie citoyenne », *Pouvoirs*.
4. CNIL, « Protéger ses données personnelles sur Facebook : les conseils pour agir », 28 janvier 2014.
5. D. LELOUP, « Piratage d'Ashley Madison : qui sont les vraies victimes ? », *Le Monde,* Pixels, 20 juillet 2015.
6. CNIL, « Données traitées par les sites de rencontre : 8 mises en demeure », 8 juillet 2015.

B – La protection des atteintes commises par les personnes publiques

7. Cour EDH, M.K. c France, 28 avril 2013, n°19522/09.
8. CC, décision n°2015-713 DC du 23 juillet 2015, *Loi relative au renseignement.*
9. CE, Ord., 13 mai 2015, *Association de défense et d'assistance juridique des intérêts des supporters et autres*, n°389816, 389861, 389866, 389899.
10. L. PEILLON, « Ménard aurait fait ses fiches ethniques ''seul'' et pour ''quelques écoles'' », *Libération*, 7 mai 2015.

I – Cadre juridique

Document 1 : Loi n° 78-17 du 6 janvier 1978 dite « informatique et liberté »

Article 1

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 2

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.
Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.
Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.
Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.
La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Article 3

I. - Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.
II. - Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander

au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

Article 4

Les dispositions de la présente loi ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

Article 5

I. - Sont soumis à la présente loi les traitements de données à caractère personnel :
1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;
2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne.
II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.

Chapitre II : Conditions de licéité des traitements de données à caractère personnel

Section 1 : Dispositions générales

Article 6

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :
1° Les données sont collectées et traitées de manière loyale et licite ;
2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;
3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Article 7

Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :
1° Le respect d'une obligation légale incombant au responsable du traitement ;
2° La sauvegarde de la vie de la personne concernée ;
3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Section 2 : Dispositions propres à certaines catégories de données

Article 8

I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.
II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :
1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;
2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;
3° Les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :
- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;
- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;
- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;
5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;

6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;
7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ;
8° Les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX.
III. - Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions du chapitre IX ne sont pas applicables.
IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues aux I et V de l'article 22 ou au II de l'article 26.

Article 9

Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre que par :
1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;
2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;
3° [*Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004* ;]
4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.

Article 10

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.
Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.
Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour

lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.

Chapitre III : La Commission nationale de l'informatique et des libertés.

Article 11

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes :
1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;
2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi.
A ce titre :
a) Elle autorise les traitements mentionnés à l'article 25, donne un avis sur les traitements mentionnés aux articles 26 et 27 et reçoit les déclarations relatives aux autres traitements ;
b) Elle établit et publie les normes mentionnées au I de l'article 24 et édicte, le cas échéant, des règlements types en vue d'assurer la sécurité des systèmes ;
c) Elle reçoit les réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;
d) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ;
e) Elle informe sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 52 ;
f) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 44, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;
g) (Abrogé)
h) Elle répond aux demandes d'accès concernant les traitements mentionnés aux articles 41 et 42 ;
3° A la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements :
a) Elle donne un avis sur la conformité aux dispositions de la présente loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel, ou à l'anonymisation de ces données, qui lui sont soumis ;
b) Elle porte une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la présente loi, au regard du respect des droits fondamentaux des personnes ;
c) Elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a

reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission ; la commission peut également déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label . Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ; elle retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites ;

4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;

A ce titre :

a) Elle est consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés. A la demande du président de l'une des commissions permanentes prévue à l'article 43 de la Constitution, l'avis de la commission sur tout projet de loi est rendu public ;

b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques ;

c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ;

d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine.

Pour l'accomplissement de ses missions, la commission peut procéder par voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.

La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission.

Document 2 : CC, décision n°2012-652 DC du 22 mars 2012 [Loi relative à la protection de l'identité]

LE CONSEIL CONSTITUTIONNEL,

Vu l'ordonnance n° 58-1067 du 7 novembre 1958 modifiée portant loi organique sur le Conseil constitutionnel ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu les observations du Gouvernement en réponse à la saisine ainsi que ses observations complémentaires produites à la demande du Conseil constitutionnel, enregistrées le 15 mars

2012 ;

Vu les observations en réplique présentées par les sénateurs requérants, enregistrées le 20 mars 2012 ;

Le rapporteur ayant été entendu ;

1. Considérant que les députés et sénateurs requérants défèrent au Conseil constitutionnel la loi relative à la protection de l'identité ; qu'ils contestent la conformité à la Constitution des dispositions de ses articles 5 et 10 ;

- SUR LES ARTICLES 5 et 10 :

2. Considérant que l'article 5 de la loi déférée prévoit la création, dans les conditions prévues par la loi du 6 janvier 1978 susvisée, d'un traitement de données à caractère personnel facilitant le recueil et la conservation des données requises pour la délivrance du passeport français et de la carte nationale d'identité, destiné à préserver l'intégrité de ces données ; que, parmi celles-ci, figurent les données contenues dans le composant électronique sécurisé de la carte nationale d'identité et du passeport dont la liste est fixée à l'article 2 de la loi, qui sont, outre l'état civil et le domicile du titulaire, sa taille, la couleur de ses yeux, deux empreintes digitales et sa photographie ;

3. Considérant que cet article 5 permet que l'identification du demandeur d'un titre d'identité ou de voyage s'effectue en interrogeant le traitement de données à caractère personnel au moyen des données dont la liste est fixée à l'article 2, à l'exception de la photographie ; qu'il prévoit également que ce traitement de données à caractère personnel peut être interrogé au moyen des deux empreintes digitales recueillies dans le traitement, en premier lieu, lors de l'établissement des titres d'identité et de voyage, en deuxième lieu, pour les besoins de l'enquête relative à certaines infractions, sur autorisation du procureur de la République ou du juge d'instruction, et, en troisième lieu, sur réquisition du procureur de la République aux fins d'établir, lorsqu'elle est inconnue, l'identité d'une personne décédée, victime d'une catastrophe naturelle ou d'un accident collectif ;

4. Considérant que l'article 6 de la loi déférée permet de vérifier l'identité du possesseur de la carte d'identité ou du passeport à partir des données inscrites sur le document d'identité ou de voyage ou sur le composant électronique sécurisé ; qu'il permet également que cette vérification soit effectuée en consultant les données conservées dans le traitement prévu à l'article 5 « en cas de doute sérieux sur l'identité de la personne ou lorsque le titre présenté est défectueux ou paraît endommagé ou altéré » ;

5. Considérant que l'article 10 permet aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales d'avoir accès au traitement de données à caractère personnel créé en application de l'article 5, pour les besoins de la prévention et de la répression des atteintes à l'indépendance de la Nation, à l'intégrité de son territoire, à sa sécurité, à la forme républicaine de ses institutions, aux moyens de sa défense

et de sa diplomatie, à la sauvegarde de sa population en France et à l'étranger et aux éléments essentiels de son potentiel scientifique et économique et des actes de terrorisme ;

6. Considérant que, selon les requérants, la création d'un fichier d'identité biométrique portant sur la quasi-totalité de la population française et dont les caractéristiques rendent possible l'identification d'une personne à partir de ses empreintes digitales porte une atteinte inconstitutionnelle au droit au respect de la vie privée ; qu'en outre, en permettant que les données enregistrées dans ce fichier soient consultées à des fins de police administrative ou judiciaire, le législateur aurait omis d'adopter les garanties légales contre le risque d'arbitraire ;

7. Considérant, en premier lieu, que l'article 34 de la Constitution dispose que la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ainsi que la procédure pénale ; qu'il appartient au législateur, dans le cadre de sa compétence, d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect des autres droits et libertés constitutionnellement protégés ; qu'il lui est à tout moment loisible d'adopter des dispositions nouvelles dont il lui appartient d'apprécier l'opportunité et de modifier des textes antérieurs ou d'abroger ceux-ci en leur substituant, le cas échéant, d'autres dispositions, dès lors que, dans l'exercice de ce pouvoir, il ne prive pas de garanties légales des exigences constitutionnelles ;

8. Considérant, en second lieu, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ;

9. Considérant que la création d'un traitement de données à caractère personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage permet de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude ; qu'elle est ainsi justifiée par un motif d'intérêt général ;

10. Considérant, toutefois, que, compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française ; que les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne ; que les dispositions de la loi déférée autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire ;

11. Considérant qu'il résulte de ce qui précède qu'eu égard à la nature des données

enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ; que, par suite, les articles 5 et 10 de la loi doivent être déclarés contraires à la Constitution ; qu'il en va de même, par voie de conséquence, du troisième alinéa de l'article 6, de l'article 7 et de la seconde phrase de l'article 8 ;

- SUR L'ARTICLE 3 :

12. Considérant que l'article 3 de la loi déférée confère une nouvelle fonctionnalité à la carte nationale d'identité ; qu'aux termes de cet article : « Si son titulaire le souhaite, la carte nationale d'identité contient en outre des données, conservées séparément, lui permettant de s'identifier sur les réseaux de communications électroniques et de mettre en oeuvre sa signature électronique. L'intéressé décide, à chaque utilisation, des données d'identification transmises par voie électronique.
« Le fait de ne pas disposer de la fonctionnalité décrite au premier alinéa ne constitue pas un motif légitime de refus de vente ou de prestation de services au sens de l'article L. 122-1 du code de la consommation ni de refus d'accès aux opérations de banque mentionnées à l'article L. 311-1 du code monétaire et financier.
« L'accès aux services d'administration électronique mis en place par l'État, les collectivités territoriales ou leurs groupements ne peut être limité aux seuls titulaires d'une carte nationale d'identité présentant la fonctionnalité décrite au premier alinéa du présent article » ;

13. Considérant que, selon l'article 34 de la Constitution, la loi fixe les règles concernant les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques et l'état et la capacité des personnes ; qu'elle détermine également les principes fondamentaux des obligations civiles et commerciales ; qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, les conditions générales dans lesquelles la carte nationale d'identité délivrée par l'État peut permettre à une personne de s'identifier sur les réseaux de communication électronique et de mettre en œuvre sa signature électronique, notamment à des fins civiles et commerciales, affectent directement les règles et les principes précités et, par suite, relèvent du domaine de la loi ;

14. Considérant que l'article 3, d'une part, permet que la carte nationale d'identité comprenne des « fonctions électroniques » permettant à son titulaire de s'identifier sur les réseaux de communication électroniques et de mettre en œuvre sa signature électronique et, d'autre part, garantit le caractère facultatif de ces fonctions ; que les dispositions de l'article 3 ne précisent ni la nature des « données » au moyen desquelles ces fonctions peuvent être mises en œuvre ni les garanties assurant l'intégrité et la confidentialité de ces données ; qu'elles ne définissent pas davantage les conditions dans lesquelles s'opère l'authentification des personnes mettant en œuvre ces fonctions, notamment lorsqu'elles sont mineures ou bénéficient d'une mesure de protection juridique ; que, par suite, le législateur a méconnu l'étendue de sa compétence ; qu'il en résulte que l'article 3 doit être déclaré contraire à la Constitution ;

15. Considérant qu'il n'y a lieu, pour le Conseil constitutionnel, de soulever d'office aucune autre question de conformité à la Constitution,

D É C I D E :

Article 1er.- Sont déclarées contraires à la Constitution les dispositions suivantes de la loi relative à la protection de l'identité :

- les articles 3, 5, 7 et 10 ;
- le troisième alinéa de l'article 6 ;
- la seconde phrase de l'article 8.

Article 2.- La présente décision sera publiée au Journal officiel de la République française.

II - Applications

A – La protection des atteintes commises par les personnes privées

Document 3 : C. RICHAUD, « Données personnelles : la schizophrénie citoyenne », *Pouvoirs*.

A croire que le dicton " Pour vivre heureux, vivons cachés " est devenu ringard ! A l'heure où l'affaire Hollande-Gayet est une question relative à la vie privée pour plus de 77 % des Français, où l'affaire Snowden scandalise la communauté internationale, Facebook célèbre ses dix ans et atteint le chiffre étourdissant de 26 millions d'utilisateurs en France.
Il est donc désormais courant d'avoir un profil Facebook et très certainement " has been " de ne pas en posséder. Il est pour ainsi dire " tendance " aujourd'hui d'exposer volontairement ses données personnelles, allant de la situation sentimentale et ses nombreuses déclinaisons, aux divers points de vue politiques et religieux. En un mot et en un clic, la sphère privée se retrouve exposée dans la sphère publique par les citoyens eux-mêmes. Avec de nombreuses conséquences : licenciements à la suite de propos exprimés sur Facebook, condamnations pour diffamation sur Internet, etc.
Finalement, les réseaux sociaux ôtent les filtres qui sont ceux de la vie en société et permettent aux citoyens cachés derrière leurs écrans d'exprimer, non pas leurs idéaux, mais leurs humeurs personnelles, politiques, religieuses. En un sens, là où le fichier " Edvige " - fichier de police créé en 2008 - a échoué, les réseaux sociaux ont réussi. La différence : Edvige était considéré comme liberticide alors que l'inscription sur les réseaux sociaux reste " tendance ".
Accentuant la confusion des sphères privée et publique, les réseaux sociaux ont réussi le pari d'infiltrer l'intimité jusque-là protégée par le citoyen en rassemblant, avec son accord, de nombreuses données personnelles. C'est par exemple la collecte par Apple des empreintes digitales pour les nouveaux iPhone 5 S !

Le décalage entre ce que les citoyens refusent d'accepter de la part de l'Etat au nom du respect de la vie privée et ce qu'ils sont prêts à livrer de leur intimité sur les réseaux sociaux marque l'apparition d'une nouvelle figure : le " citoyen 2.0 ".
Evidemment, la conception de ce qui relève du privé est propre à chaque individu, mais comment protéger ce " citoyen 2.0 " de lui-même ? En réalité, l'arsenal juridique et constitutionnel encadrant les abus relatifs à la conservation et la réutilisation des données personnelles au nom du respect de la vie privée ne semble plus adapté aux internautes qui voient dans les réseaux sociaux un cadre propice à la réalisation de leur liberté d'expression aux dépens du respect de leur vie privée.
Ainsi, quand le Conseil constitutionnel encadre l'enregistrement au Fichier national automatisé des empreintes digitales des personnes condamnées pour des infractions particulières le 16 septembre 2010, le " citoyen 2.0 " achète un iPhone 5S. Quand le juge limite le traitement des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté le 29 juillet 2004, le " citoyen 2.0 " poste sur les réseaux sociaux le procès-verbal de sa condamnation. Enfin, quand le Conseil constitutionnel censure la création d'un registre national des crédits aux particuliers pouvant toucher plus de 12 millions de personnes en France le 13 mars, le " citoyen 2.0 " expose sa situation financière sur Facebook.
Un vent de schizophrénie souffle. D'un côté, le " citoyen 1.0 " demeure attaché aux principes du respect de ses données personnelles et de sa vie privée au travail, de l'autre, ce même citoyen, version 2.0, est prêt à sacrifier ses droits sur l'autel de la popularité et de l'audience. Un " like " du citoyen 2.0 est-il compatible avec un " dislike " du citoyen 1.0 ? La réponse est sur votre profil Facebook.

Document 4 : CNIL, « Protéger ses données personnelles sur Facebook : les conseils pour agir », 28 janvier 2014

Les 18 millions d'utilisateurs qui utilisent quotidiennement Facebook en France peuvent parfois connaître des déconvenues : piratage de compte, diffusion de photos gênantes, difficulté à supprimer un compte, etc. À l'occasion de la journée européenne de la protection des données, la CNIL met en ligne un espace d'information dédié à Facebook sur sa page officielle.
Les internautes pourront trouver les réponses aux questions les plus courantes et aux problèmes les plus souvent rencontrés sur le réseau social. Ces questions-réponses prennent la forme d'un album photo, et proposent des conseils pratiques pour exercer ses droits " informatique et libertés ". Chacun peut commenter ces conseils, les partager et aussi suggérer de nouveaux cas pratiques.
Quelques conseils généraux

- Vous êtes concerné par une atteinte à votre vie privée ? Premier réflexe : le signalement auprès de Facebook. N'oubliez pas de conserver des preuves de ce signalement en effectuant des copies écran. Elles pourront vous servir pour adresser, le cas échéant, une plainte à la CNIL en cas de réponse incomplète, insatisfaisante, voire d'absence de réponse.
- Vous êtes victime de cyber-harcèlement ? Ce type d'agissement est susceptible de

constituer une infraction pénale. Dans ce cas, il faut adresser une plainte auprès des services de police.

La liste des conseils à partager auprès de votre réseau d'amis :

- Usurpation/réputation
- Comptes piratés/bloqués
- Diffusion de photo

- Comptes de personnes décédées
- Profil ou publications supprimés par Facebook
- Dénonciations de profils
- Gestion des paramètres de confidentialité

A propos de l'éducation au numérique

La création de ce nouvel espace d'informations pratiques participe ainsi de l'éducation au numérique, initiative qui rassemble un collectif de plus de 50 organismes issus de la société civile, du monde de l'éducation et de la recherche, des fédérations professionnelles, des institutions nationales et internationales. Ces organismes se sont unis pour faire de l'éducation au numérique une " grande cause nationale " en 2014. Un dossier de candidature a été déposé auprès des services du Premier ministre début janvier.

Document 5 : D. LELOUP, « Piratage d'Ashley Madison : qui sont les vraies victimes ? », 8 juillet 2015.

Il n'aura pas fallu longtemps. Vingt-quatre heures à peine après la révélation de la publication en ligne de la base de données des utilisateurs d'Ashley Madison, un important site de rencontres adultères, les noms et les témoignages d'utilisateurs – essentiellement des hommes – affluent dans la presse américaine et sur les réseaux sociaux.

Les données de 33 millions de comptes – qui comportaient parfois des informations très sensibles, comme les préférences sexuelles ou le numéro de téléphone – sont donc dans la nature. Et deux jours plus tard, jeudi 20 août, des pirates informatiques ont de nouveau publié une série de documents, cette fois sans information sur les utilisateurs du site, mais avec un fichier contenant possiblement des mails de Noël Biderman, le PDG d'Avid Life Media, propriétaire d'Ashley Madison. Ce qui tendrait à prouver que les documents publiés étaient authentiques.

Même si un grand nombre de comptes étaient faux, ou liés à des adresses email jetables, cela fait beaucoup. Parmi les personnes dont le nom est apparu figurent quelques personnalités publiques – un député, un activiste américain des valeurs familiales…

Que disent les personnes dont les données ont été publiées ? Le site américain Fusion en a contacté une vingtaine. « *Deux ont nié avoir jamais utilisé le site. Deux ou trois étaient furieux, en partie parce qu'ils n'avaient jamais rien tiré de leur inscription ; ils m'ont dit que le site était une arnaque, plein de faux profils de jolies femmes. Certains m'ont dit qu'ils s'étaient inscrits à une époque où ils étaient célibataires et cherchaient une aventure d'un soir, ou par curiosité. Certains disent s'être inscrits à un moment où leur couple battait de*

l'aile et que la situation s'était depuis arrangée, mais qu'ils craignaient que le piratage rouvre de vieilles blessures. Quelques-uns m'ont dit que c'était probablement la fin de leur mariage. »

L'une des personnes citées, Tom (un nom d'emprunt), ne sait pas s'il doit regretter de s'être inscrit. « *C'est une question difficile. J'étais très frustré à l'époque. Mais ça ne justifie pas ce que j'ai fait. Les répercussions* [de ce piratage] *sont gigantesques pour moi. Mais je ne peux m'en prendre qu'à moi-même.* »

Responsabilité d'Avid Life Media

A lui-même ? Sur les réseaux sociaux, des milliers de messages abondent dans le sens de Tom. Les « bien fait » s'ajoutent aux messages de félicitations pour les hackers de The Impact Team qui ont revendiqué le piratage. Pourtant, dans un message accompagnant les gigaoctets de données d'utilisateurs qu'ils ont publiés, Impact Team affirme elle-même que la responsabilité de cet étalage en plein jour est à chercher du côté d'Avid Life Media (ALM), le groupe qui édite Ashley Madison et d'autres sites de rencontres. *« Vous vous êtes retrouvé dans ce fichier ? C'est la faute d'ALM qui vous a menti. Portez plainte et réclamez des dommages et intérêts. Et continuez votre vie. Retenez la leçon et faites pénitence. C'est gênant aujourd'hui, mais ça passera. »*

La manière dont les fichiers ont été piratés est encore inconnue – l'enquête ouverte par le FBI devra notamment déterminer comment un piratage d'une telle ampleur, qui a atteint non seulement la base de données des utilisateurs mais aussi le réseau interne de l'entreprise et ses documents confidentiels, s'est déroulé. Mais les données publiées en ligne tendent à montrer qu'ALM avait pris quelques précautions de base pour protéger ses utilisateurs. Les mots de passe, notamment, n'étaient pas stockés « en clair » mais étaient protégés par un chiffrement plutôt robuste – une pratique de sécurité basique, mais que certains de ses concurrents n'avaient pas mise en place, comme l'ont montré de précédents piratages.

Des millions d'anonymes

Mais quand bien même ALM aurait insuffisamment protégé les données de ses clients et utilisateurs, leur publication en ligne reste de la responsabilité des pirates. Il y a un an presque jour pour jour, la publication de milliers de photographies suggestives de célébrités, volées sur leurs comptes iCloud, faisait scandale. Là aussi, les victimes – majoritairement des femmes – étaient pointées du doigt, suspectées de « *l'avoir bien cherché* » parce qu'elles avaient osé prendre des photographies dénudées d'elles-mêmes. Là aussi, les pratiques de personnes majeures et consentantes, dans un cadre privé, étaient dénoncées sur la place publique comme « contraires à la morale » et aboutissaient à mettre les victimes dans la position des coupables.

Le fait que quelques noms de personnalités publiques aient déjà été retrouvés dans la base de données mise en ligne ne saurait occulter le fait que des millions d'anonymes y figurent également. Et que les victimes du piratage ne correspondent pas nécessairement toutes à l'archétype du riche mari Américain coureur de jupons – et que les conséquences seront très variables en fonction des cas. Quid, par exemple, du millier d'utilisateurs du site qui se sont inscrits avec une adresse email en. sa – l'extension de l'Arabie saoudite – un pays

où l'adultère peut être puni de coups de fouet ? Quelles auraient été les réactions si la liste des utilisateurs de l'application populaire de rencontres gay Grindr avait été publiée ?

Dans tous les cas, la publication sauvage de données personnelles de millions de personnes est un acte irresponsable et une atteinte à la vie privée, qui est aussi un droit inaliénable à faire des choses que la morale réprouve tant que la loi est respectée. Et cette publication ne met pas seulement en danger des couples et des mariages : cette base de données fournit un outil très pratique aux escrocs, maîtres-chanteurs, pirates en herbe et diffuseurs de spam en tous genres.

Demandes de rançon

Ashley Madison et sa maison mère ALM avaient des pratiques plus que douteuses : faux profils, suppression incomplète des données des utilisateurs le souhaitant – alors même qu'il s'agissait là d'un service payant. Le groupe édite aussi un site qui flirte allégrement avec les limites de la prostitution, establishedmen.com. Mais il est difficile de leur donner tort lorsqu'ils affirment que *« le ou les criminels impliqués dans ces actions se sont autoproclamés juges de moralité, jury et bourreau, et cherchent à imposer leur propre conception de la vertu à l'ensemble de la société* ».

Dans leur premier communiqué, mi-juillet, The Impact Team annonçait avoir mis la main sur la base de données du site, et menaçait de la rendre publique si ALM ne fermait pas ses différents services de rencontre. Le message dénonçait aussi les « *salauds de menteurs* » inscrits sur Ashley Madison. Mais la publication des informations un mois après ce premier message laisse également planer le doute sur les motivations réelles des hackeurs et l'importance qu'ont joué leurs « convictions morales » dans ce gigantesque déballage public.

Les personnes qui cherchent à dénoncer des pratiques, quelles qu'elles soient, en publiant des documents, donnent rarement un avertissement. WikiLeaks ne pose pas d'ultimatums aux gouvernements auquel il s'attaque en publiant des documents confidentiels : il publie les documents. L'ultimatum n'a de sens que lorsque l'on cherche à obtenir une contrepartie financière, comme lors des piratages récents des sites AdultFriendFinder et TopFace, qui avaient donné lieu à des demandes de rançon.

Document 6 : CNIL, « Données traitées par les sites de rencontre : 8 mises en demeure », 8 juillet 2015.

A la suite de contrôles effectués auprès de plusieurs sites de rencontre ayant révélé de nombreux manquements à la loi Informatique et Libertés, notamment sur les informations sensibles fournies par leurs clients, la Présidente de la CNIL met en demeure huit acteurs du secteur.

De plus en plus de Français se rendent sur les sites de rencontre. La plupart de ces sites offrent à leurs utilisateurs une recherche de partenaires très ciblée : par communauté sociale, ethnique ou religieuse, par localisation géographique, en fonction de l'apparence physique,

des pratiques sexuelles ou des opinions politiques, etc. Le nombre important des utilisateurs ainsi que la quantité des données traitées et leur sensibilité ont conduit la CNIL à inscrire les sites de rencontre dans son programme annuel des contrôles pour 2014. 13 sites ont été contrôlés : Meetic, Attractive World, Adopte un mec, Easyflirt, Rencontre obèse, Destidyll, Forcegay, Mektoube, Jdream, Feujworld, Marmite love, Gauche rencontre, Celibest. De nombreux manquements à la loi informatique et libertés ont été constatés, notamment :

- les sites ne recueillent pas le consentement exprès des personnes pour la collecte de données sensibles (par exemple : données relatives à la vie et aux pratiques sexuelles, aux origines ethniques, aux convictions et pratiques religieuses, aux opinions politiques). Or, il est important que les internautes aient conscience de la protection attachée à ces données qui révèlent des éléments-clés de leur intimité. Ce recueil pourrait prendre la forme d'une case à cocher permettant de sensibiliser les internautes sur la sensibilité des données qu'ils renseignent ;

Exemple de case à cocher *Les informations relatives à vos convictions politiques, croyances et pratiques religieuses, orientations et pratiques sexuelles, collectées pour l'inscription à ce site de rencontres, constituent des informations sensibles. J'accepte que ces données soient traitées par le site XXX*

- les sites ne procèdent pas à la suppression des données des membres ayant demandé leur désinscription ou ayant cessé d'utiliser leurs comptes depuis une longue durée ;
- ils mettent en œuvre des fichiers afin d'exclure des personnes de l'accès au service sans avoir procédé à des demandes d'autorisation auprès de la CNIL ;
- ils n'informent pas correctement les internautes de leurs droits (accès, suppression, rectification) ainsi que des conditions dans lesquelles des cookies sont déposés sur leur ordinateur.

La Présidente de la CNIL a décidé de mettre en demeure les huit organismes responsables de ces treize sites ayant fait l'objet des contrôles de se mettre en conformité sur ces différents points. Cette mise en demeure a été rendue publique par le bureau de la CNIL compte tenu de la sensibilité des données en cause et du nombre de personnes concernées. La CNIL rappelle que ces mises en demeure ne sont pas des sanctions. En effet, aucune suite ne sera donnée à ces procédures si les sociétés se conforment à la loi dans le délai de trois mois. Dans ce cas, la clôture de chacune des procédures fera également l'objet d'une publicité. Si les sociétés ne se conforment pas à cette mise en demeure dans le délai imparti, la Présidente pourra désigner un rapporteur qui, le cas échéant, pourra établir un rapport proposant à la formation restreinte de la CNIL, chargée de sanctionner les manquements à la loi Informatique et Libertés, de prononcer une sanction à leur égard. Accompagnant cette mise en demeure, la CNIL publie des conseils à destination des particuliers.

B – La protection des atteintes commises par les personnes publiques

Document 7 : Cour EDH, M. K c France, 28 avril 2013, n°19522/09.

PROCÉDURE

1. A l'origine de l'affaire se trouve une requête (n° 19522/09) dirigée contre la République française et dont un ressortissant de cet Etat, M. M. K. (« le requérant »), a saisi la Cour le 28 février 2009 en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »).

2. Le requérant, qui a été admis au bénéfice de l'assistance judiciaire, a été représenté par Me C. Meyer, avocat à Strasbourg. Le gouvernement français (« le Gouvernement ») est représenté par son agent, Mme E. Belliard, directrice des affaires juridiques au ministère des Affaires étrangères.

3. Le requérant allègue en particulier une violation de l'article 8 de la Convention, en raison de la conservation de données le concernant au fichier automatisé des empreintes digitales.

4. Le 8 mars 2011, la requête a été communiquée au Gouvernement.

EN FAIT

I. LES CIRCONSTANCES DE L'ESPÈCE

5. Le requérant est né en 1972 et réside à Paris.

6. Le 10 février 2004, une enquête fut ouverte à l'encontre du requérant pour vol de livres. Les services d'enquête prélevèrent ses empreintes digitales.

7. Par un arrêt du 15 février 2005, sur appel d'un jugement rendu le 28 avril 2004 par le tribunal correctionnel de Paris, la cour d'appel de Paris relaxa le requérant.

8. Le 28 septembre 2005, le requérant fut placé en garde à vue dans le cadre d'une enquête de flagrance, également pour vol de livres. Il fit à nouveau l'objet d'un prélèvement d'empreintes digitales.

9. Le 2 février 2006, cette procédure fut classée sans suite par le procureur de la République de Paris.

10. Les empreintes relevées lors de ces procédures furent enregistrées au fichier automatisé des empreintes digitales (« FAED »).

11. Par une lettre du 21 avril 2006, le requérant demanda au procureur de la République de Paris que ses empreintes soient effacées du FAED.

12. Le 31 mai 2006, le procureur de la République fit procéder uniquement à l'effacement des prélèvements effectués lors de la première procédure. Il fit valoir que la conservation d'un exemplaire des empreintes du requérant se justifiait dans l'intérêt de celui-ci, en permettant d'exclure sa participation en cas de faits commis par un tiers usurpant son identité.

13. Le 26 juin 2006, le requérant forma un recours devant le juge des libertés et de la détention du tribunal de grande instance de Paris.

14. Par une ordonnance du 25 août 2006, le juge des libertés et de la détention rejeta sa demande. Il estima que la conservation des empreintes était de l'intérêt des services d'enquête, leur permettant de disposer d'un fichier ayant le plus de références possibles. Le juge ajouta que cette mesure ne causait aucun grief au requérant, compte tenu de la confidentialité du fichier, qui excluait toute conséquence sur la vie sociale ou personnelle de l'intéressé.

15. Le 21 décembre 2006, le président de la chambre de l'instruction de la cour d'appel de Paris confirma cette ordonnance.

16. Par un arrêt du 1er octobre 2008, la Cour de cassation rejeta le pourvoi du requérant en considérant, la procédure étant écrite, qu'il avait été mis en mesure de faire valoir son argumentation et de prendre connaissance de l'opposition motivée du ministère public. Elle ajouta que les pièces de la procédure lui permettaient de s'assurer que la demande avait été traitée conformément aux textes légaux et conventionnels invoqués par le requérant, parmi lesquels figurait l'article 8 de la Convention.

[…]
EN DROIT

I. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION

20. Le requérant allègue une atteinte à son droit au respect de sa vie privée, en raison de la conservation de données le concernant au fichier automatisé des empreintes digitales. Il invoque l'article 8 de la Convention, ainsi libellé :

« 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. »

21. Le Gouvernement s'oppose à cette thèse.

A. Sur la recevabilité

22. La Cour constate que ce grief n'est pas manifestement mal fondé au sens de l'article 35 § 3 (a) de la Convention. La Cour relève par ailleurs qu'il ne se heurte à aucun autre motif

d'irrecevabilité. Il convient donc de le déclarer recevable.

[…]

2. Appréciation de la Cour

a) L'existence d'une ingérence

29. La Cour rappelle que la conservation, dans un fichier des autorités nationales, des empreintes digitales d'un individu identifié ou identifiable constitue une ingérence dans le droit au respect de la vie privée (S. et Marper, précité, § 86).

b) Justification de l'ingérence

i. Base légale

30. Une telle ingérence doit donc être prévue par la loi, ce qui suppose l'existence d'une base en droit interne, qui soit compatible avec la prééminence du droit. 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 (voir, entre autres, Malone c. Royaume-Uni, 2 août 1984, §§ 66-68, série A n^{o} 82, Rotaru c. Roumanie [GC], no 28341/95, § 55, CEDH 2000-V, et S. et Marper, précité, § 95). 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 (voir, parmi d'autres, Hassan et Tchaouch c. Bulgarie [GC], n^{o} 30985/96, § 84, CEDH 2000-XI, et S. et Marper, précité, § 96).

31. En l'espèce, la Cour constate que l'ingérence est prévue par la loi, à savoir l'article 55-1 du code de procédure pénale et le décret n^{o} 87-249 du 8 avril 1987 modifié. Quant à la question de savoir si la législation en cause est suffisamment claire et précise s'agissant des conditions de mémorisation, d'utilisation et d'effacement des données personnelles, la Cour note que le requérant évoque ces problèmes dans le cadre de ses développements sur la proportionnalité de l'ingérence. En tout état de cause, elle estime que ces aspects sont en l'espèce étroitement liés à la question plus large de la nécessité de l'ingérence dans une société démocratique et qu'un tel contrôle de la « qualité » de la loi dans la présente affaire renvoie à l'analyse ci-après de la proportionnalité de l'ingérence litigieuse (S. et Marper, précité, § 99).

ii. But légitime

32. La Cour note ensuite que l'ingérence vise un but légitime : la détection et, par voie de conséquence, la prévention des infractions pénales (S. et Marper, précité, § 100).

iii. Nécessité de l'ingérence

α) Les principes généraux

33. Il reste donc à déterminer si l'ingérence litigieuse peut être considérée comme « nécessaire dans une société démocratique », ce qui commande qu'elle réponde à un « besoin social impérieux » et, en particulier, qu'elle soit proportionnée au but légitime poursuivi et que les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants » (S. et Marper, précité, § 101).

34. S'il appartient tout d'abord aux autorités nationales de juger 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 S. et Marper, précité). Une certaine marge d'appréciation, dont l'ampleur varie et dépend d'un certain nombre d'éléments, notamment de la nature des activités en jeu et des buts des restrictions (voir, notamment, Smith et Grady c. Royaume-Uni, nos 33985/96 et 33986/96, § 88, CEDH 1999-VI ; Gardel c. France, n° 16428/05, B.B. c. France, n° 5335/06, et M.B. c. France, n° 22115/06, 17 décembre 2009, respectivement §§ 60, 59 et 51), est donc laissée en principe aux Etats dans ce cadre (voir, parmi beaucoup d'autres, Klass et autres c. Allemagne, 6 septembre 1978, § 49, série A n° 28). 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 S. et Marper, précité, § 102). 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-I, S. et Marper, précité, et Gardel, B.B. et M.B., précités, respectivement §§ 61, 60 et 52). 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-XIII).

35. La protection des données 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 caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (S. et Marper, précité, § 103, et Gardel, B.B. et M.B., précités, §§ 62, 61 et 53 respectivement). A l'instar de ce qu'elle a dit dans l'arrêt S. et Marper (précité), 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. Le droit interne doit notamment assurer que ces données soient pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles soient 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. Il doit aussi contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (ibidem).

36. Enfin, il appartient à la Cour d'être particulièrement attentive au risque de stigmatisation de personnes qui, à l'instar du requérant, n'ont été reconnues coupables d'aucune infraction et

sont en droit de bénéficier de la présomption d'innocence, alors que leur traitement est le même que celui de personnes condamnées. Si, de ce point de vue, la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donne pas l'impression de ne pas être considérés comme innocents (S. et Marper, précité, § 122).

β) L'application des principes susmentionnés au cas d'espèce

37. En l'espèce, la mesure litigieuse, qui n'emporte en elle-même aucune obligation à la charge du requérant, obéit à des modalités de consultation suffisamment encadrées, qu'il s'agisse des personnes habilitées à consulter le fichier ou du régime d'autorisation auxquelles sont soumises les opérations d'identification qui correspondent à la finalité du fichier (voir, a contrario, Khelili c. Suisse, n° 16188/07, § 64, 18 octobre 2011).

38. La Cour observe qu'il en va différemment du régime de collecte et de conservation des données.

39. En effet, la Cour note d'emblée que la finalité du fichier, nonobstant le but légitime poursuivi, a nécessairement pour résultat l'ajout et la conservation du plus grand nombre de noms possibles, ce que confirme la motivation retenue par le juge des libertés et de la détention dans son ordonnance du 25 août 2006 (paragraphe 14 ci-dessus).

40. Elle relève par ailleurs que le refus du procureur de la République de faire procéder à l'effacement des prélèvements effectués lors de la seconde procédure était motivé par la nécessité de préserver les intérêts du requérant, en permettant d'exclure sa participation en cas d'usurpation de son identité par un tiers (paragraphe 12 ci-dessus). Or, outre le fait qu'un tel motif ne ressort pas expressément des dispositions de l'article 1er du décret litigieux, sauf à en faire une interprétation particulièrement extensive, la Cour estime que retenir l'argument tiré d'une prétendue garantie de protection contre les agissements des tiers susceptibles d'usurper une identité reviendrait, en pratique, à justifier le fichage de l'intégralité de la population présente sur le sol français, ce qui serait assurément excessif et non pertinent.

41. De plus, à la première fonction du fichier qui est de faciliter la recherche et l'identification des auteurs de crimes et de délits, le texte en ajoute une seconde, à savoir « faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie » dont il n'est pas clairement indiqué qu'elle se limiterait aux crimes et délits. En visant également « les personnes, mises en cause dans une procédure pénale, dont l'identification s'avère nécessaire » (article 3, 2° du décret), il est susceptible d'englober de facto toutes les infractions, y compris les simples contraventions dans l'hypothèse où cela permettrait d'identifier des auteurs de crimes et de délits selon l'objet de l'article 1 du décret (paragraphe 17 ci-dessus). En tout état de cause, les circonstances de l'espèce, relatives à des faits de vol de livres classés sans suite, témoignent de ce que le texte s'applique pour des infractions mineures. La présente affaire se distingue ainsi clairement de celles qui concernaient spécifiquement des infractions aussi graves que la criminalité organisée (S. et Marper, précité) ou des agressions sexuelles (Gardel, B.B. et M.B., précités).

42. En outre, la Cour note que le décret n'opère aucune distinction fondée sur l'existence ou non d'une condamnation par un tribunal, voire même d'une poursuite par le ministère public.

Or, dans son arrêt S. et Marper, la Cour a souligné le risque de stigmatisation, qui découle du fait que les personnes qui avaient respectivement bénéficié d'un acquittement et d'une décision de classement sans suite - et étaient donc en droit de bénéficier de la présomption d'innocence - étaient traitées de la même manière que des condamnés (§ 22). La situation dans la présente affaire est similaire sur ce point, le requérant ayant bénéficié d'une relaxe dans le cadre d'une première procédure, avant de voir les faits reprochés par la suite classés sans suite.

43. Aux yeux de la Cour, les dispositions du décret litigieux relatives aux modalités de conservation des données n'offrent pas davantage une protection suffisante aux intéressés.

44. S'agissant tout d'abord de la possibilité d'effacement de ces données, elle considère que le droit de présenter à tout moment une demande en ce sens au juge risque de se heurter, pour reprendre les termes de l'ordonnance du 25 août 2006, à l'intérêt des services d'enquêtes qui doivent disposer d'un fichier ayant le plus de références possibles (paragraphe 14 ci-dessus). Partant, les intérêts en présence étant - ne serait-ce que partiellement - contradictoires, l'effacement, qui n'est au demeurant pas un droit, constitue une garantie « théorique et illusoire » et non « concrète et effective ».

45. La Cour constate que si la conservation des informations insérées dans le fichier est limitée dans le temps, cette période d'archivage est de vingt-cinq ans. Compte tenu de son précédent constat selon lequel les chances de succès des demandes d'effacement sont pour le moins hypothétiques, une telle durée est en pratique assimilable à une conservation indéfinie ou du moins, comme le soutient le requérant, à une norme plutôt qu'à un maximum.

46. En conclusion, la Cour estime que l'Etat défendeur a outrepassé sa marge d'appréciation en la matière, le régime de conservation dans le fichier litigieux des empreintes digitales de personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué au requérant en l'espèce, ne traduisant pas un juste équilibre entre les intérêts publics et privés concurrents en jeu. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique.

47. Partant, il y a eu violation de l'article 8 de la Convention.

Document 8 : CC, décision n°2015-713 DC du 23 juillet 2015, [Loi relative au renseignement]

[…]

- SUR LES NORMES DE RÉFÉRENCE :

2. Considérant qu'en vertu de l'article 34 de la Constitution, il appartient au législateur de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de

droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis ; qu'au nombre de ces derniers figurent le droit au respect de la vie privée, l'inviolabilité du domicile et le secret des correspondances, protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789 ;

3. Considérant qu'en vertu de l'article 5 de la Constitution, le Président de la République est le garant de l'indépendance nationale et de l'intégrité du territoire ; qu'aux termes du premier alinéa de l'article 20 : « Le Gouvernement détermine et conduit la politique de la Nation » ; qu'en vertu de l'article 21, le Premier ministre « dirige l'action du Gouvernement » et « est responsable de la Défense nationale » ; que le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire ;

4. Considérant qu'aux termes de l'article 66 de la Constitution : « Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi » ;

5. Considérant qu'aux termes de l'article 16 de la Déclaration de 1789 : « Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution » ; que sont garantis par cette disposition le droit des personnes intéressées à exercer un recours juridictionnel effectif, le droit à un procès équitable ainsi que le principe du contradictoire ;

[…]

En ce qui concerne l'article L. 821-6 du code de la sécurité intérieure :

27. Considérant que l'article L. 821-6 du code de la sécurité intérieure institue une procédure dérogatoire d'installation, d'utilisation et d'exploitation des appareils ou dispositifs techniques de localisation en temps réel d'une personne, d'un véhicule ou d'un objet, d'identification d'un équipement terminal ou du numéro d'abonnement ainsi que de localisation de cet équipement ou d'interception des correspondances émises ou reçues par cet équipement, en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération ultérieurement ; que cette procédure permet aux agents individuellement désignés et habilités d'installer, utiliser et exploiter sans autorisation préalable ces appareils ou dispositifs techniques ; que le Premier ministre, le ministre concerné et la commission nationale de contrôle des techniques de renseignement en sont informés sans délai et par tout moyen ; que le Premier ministre peut ordonner à tout moment d'interrompre la mise en œuvre de la technique et de détruire sans délai les renseignements collectés ; qu'une autorisation doit être ensuite délivrée par le Premier ministre, dans un délai de quarante-huit heures, après avis rendu par la commission au vu des éléments de motivation mentionnés à l'article L. 821-4 du même code et de ceux justifiant le recours à la procédure d'urgence ;

28. Considérant, d'une part, que la procédure prévue à l'article L. 821-6 peut être utilisée pour la mise en place des techniques de recueil de renseignement prévues par les articles L. 851-5, L. 851-6 et par le paragraphe II de l'article L. 852-1 du code de la sécurité intérieure ; que ces

procédures permettent à l'autorité administrative d'utiliser un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet, ou de recueillir ou d'intercepter, au moyen d'un appareil ou d'un dispositif, sans le consentement de leur auteur les données de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés et les correspondances émises ou reçues par un équipement terminal ;
29. Considérant, d'autre part, qu'à l'inverse des autres procédures dérogatoires, y compris celle instituée par l'article L. 821-5 du même code, la procédure prévue par l'article L. 821-6 permet de déroger à la délivrance préalable d'une autorisation par le Premier ministre ou par l'un de ses collaborateurs directs habilités au secret de la défense nationale auxquels il a délégué cette attribution, ainsi qu'à la délivrance d'un avis préalable de la commission nationale de contrôle des techniques de renseignement ; qu'elle ne prévoit pas non plus que le Premier ministre et le ministre concerné doivent être informés au préalable de la mise en œuvre d'une technique dans ce cadre ; que, par suite, les dispositions de l'article L. 821-6 portent une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances ; que les dispositions de l'article L. 821-6 du code de la sécurité intérieure doivent être déclarées contraires à la Constitution ;

30. Considérant que, par voie de conséquence, la dernière phrase du premier alinéa de l'article L. 821-7 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi déférée, qui est indissociable des dispositions de l'article L. 821-6, doit également être déclarée contraire à la Constitution ; qu'il en va de même des mots : « et L. 821-6 » au septième alinéa de l'article L. 833-9 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi déférée ;
[…]

En ce qui concerne les articles L. 851-1 et L. 851-2 du code de la sécurité intérieure :

52. Considérant que l'article L. 851-1 du code de la sécurité intérieure reprend la procédure de réquisition administrative de données techniques de connexion prévue auparavant à l'article L. 246-1 du même code autorisant l'autorité administrative à recueillir des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, auprès des opérateurs de communications électroniques, auprès des personnes offrant, au titre d'une activité professionnelle principale ou accessoire, au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau et auprès de celles qui assurent, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ; que, par exception aux dispositions de l'article L. 821-2 du même code, lorsque la demande sera relative à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ou au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, elle sera directement transmise à la commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement ;

53. Considérant que l'article L. 851-2 du code de la sécurité intérieure permet à l'administration, pour les seuls besoins de la prévention du terrorisme, de recueillir en temps réel, sur les réseaux des opérateurs et personnes mentionnés à l'article L. 851-1, les informations ou documents mentionnés à ce même article relatifs à une personne préalablement identifiée comme présentant une menace ;

54. Considérant que les députés requérants font valoir que le législateur a méconnu l'étendue de sa compétence en ne définissant pas suffisamment les données de connexion pouvant faire l'objet d'un recueil par les autorités administratives et que la procédure porte une atteinte disproportionnée au droit au respect de la vie privée compte tenu de la nature des données pouvant être recueillies, de l'ampleur des techniques pouvant être utilisées et des finalités poursuivies ;

55. Considérant, en premier lieu, que l'autorisation de recueil de renseignement prévue par les articles L. 851-1 et L. 851-2 porte uniquement sur les informations ou documents traités ou conservés par les réseaux ou services de communications électroniques des personnes mentionnées au considérant 52 ; que selon les dispositions du paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées par les opérateurs de communications électroniques et les personnes offrant au public une connexion permettant une telle communication portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, les données conservées par les personnes offrant un accès à des services de communication en ligne et celles assurant le stockage de diverses informations pour mise à disposition du public par ces services sont celles de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées ;

56. Considérant, en second lieu, que cette technique de recueil de renseignement est mise en œuvre dans les conditions et avec les garanties rappelées au considérant 51 ; qu'elle ne pourra être mise en œuvre que pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure ; qu'elle est autorisée pour une durée de quatre mois renouvelable conformément à l'article L. 821-4 du même code ; qu'en outre, lorsque le recueil des données a lieu en temps réel, il ne pourra être autorisé que pour les besoins de la prévention du terrorisme, pour une durée de deux mois renouvelable, uniquement à l'égard d'une personne préalablement identifiée comme présentant une menace et sans le recours à la procédure d'urgence absolue prévue à l'article L. 821-5 du même code ; que, par suite, le législateur a assorti la procédure de réquisition de données techniques de garanties propres à assurer entre, d'une part, le respect de la vie privée des personnes et, d'autre part, la prévention des atteintes à l'ordre public et celle des infractions, une conciliation qui n'est pas manifestement déséquilibrée ;

57. Considérant qu'il résulte de tout ce qui précède que les articles L. 851-1 et L. 851-2 du

code de la sécurité intérieure doivent être déclarés conformes à la Constitution ;
. En ce qui concerne l'article L. 851-3 du code de la sécurité intérieure :

58. Considérant que l'article L. 851-3 du code de la sécurité intérieure prévoit qu'il pourra être imposé aux opérateurs et aux personnes mentionnées à l'article L. 851-1 du même code la mise en œuvre, sur leur réseau, de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ; que ces traitements automatisés utiliseront exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles répondant à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent ; que, lorsque ces traitements détecteront des données susceptibles de caractériser l'existence d'une menace terroriste, l'identification de la ou des personnes concernées et le recueil des données y afférentes pourront être autorisés par le Premier ministre ou par l'une des personnes déléguées par lui ;

59. Considérant que les députés requérants soutiennent que, compte tenu du nombre de données susceptibles d'être contrôlées et de l'insuffisance des garanties concernant les « faux positifs », la technique prévue par ces dispositions porte une atteinte disproportionnée au droit au respect de la vie privée ;

60. Considérant que la technique de recueil de renseignement prévue à l'article L. 851-3 est mise en œuvre dans les conditions et avec les garanties rappelées au considérant 51 ; qu'elle ne peut être mise en œuvre qu'aux fins de prévention du terrorisme ; que tant le recours à la technique que les paramètres du traitement automatisé sont autorisés après avis de la commission nationale de contrôle des techniques de renseignement ; que la première autorisation d'utilisation de cette technique est délivrée pour une durée limitée à deux mois et que la demande de renouvellement doit comporter un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements ; que les traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent ; que, lorsqu'une donnée détectée par le traitement automatisé est susceptible de caractériser l'existence d'une menace terroriste, une nouvelle autorisation du Premier ministre sera nécessaire, après avis de la commission nationale de contrôle des techniques de renseignement, afin d'identifier la personne concernée ; que ces données sont exploitées dans un délai de soixante jours à compter de ce recueil et sont détruites à l'expiration de ce délai sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste ; que l'autorisation d'usage de cette technique ne peut être délivrée selon la procédure d'urgence absolue prévue à l'article L. 821-5 ; que, par suite, ces dispositions ne portent pas une atteinte manifestement disproportionnée au droit au respect de la vie privée ; que les dispositions de l'article L. 851-3 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;
. En ce qui concerne les articles L. 851-4, L. 851-5 et L. 851-6 du code de la sécurité intérieure :

61. Considérant que l'article L. 851-4 du code de la sécurité intérieure autorise l'autorité

administrative à requérir des opérateurs la transmission en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés mentionnés à l'article L. 851-1 ; que, selon l'article L. 851-5, l'autorité administrative peut utiliser un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet ; que l'article L. 851-6 prévoit la possibilité pour cette même autorité de recueillir, au moyen d'un appareil ou d'un dispositif permettant d'intercepter, sans le consentement de leur auteur, des paroles ou des correspondances émises, transmises ou reçues par la voie électronique ou d'accéder à des données informatiques, les données de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ;

62. Considérant que, selon les députés requérants, au regard des finalités justifiant leur mise en œuvre, ces techniques portent une atteinte disproportionnée au droit au respect de la vie privée ;

63. Considérant que les techniques de recueil de renseignement précitées sont mises en œuvre dans les conditions et avec les garanties rappelées au considérant 51 et pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure ; que lorsque la mise en œuvre de la technique prévue à l'article L. 851-5 impose l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3 ; que l'autorisation d'utilisation de la technique prévue à l'article L. 851-6 est délivrée pour une durée de deux mois renouvelable dans les mêmes conditions de durée ; que les appareils ou dispositifs utilisés dans le cadre de cette dernière technique font l'objet d'une inscription dans un registre spécial tenu à la disposition de la commission nationale de contrôle des techniques de renseignement ; que le nombre maximal de ces appareils ou dispositifs pouvant être utilisés simultanément est arrêté par le Premier ministre, après avis de cette commission ; que les informations ou documents recueillis par ces appareils ou dispositifs doivent être détruits dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre et, en tout état de cause, dans un délai maximal de quatre-vingt-dix jours à compter de leur recueil ; que, dans ces conditions, les dispositions critiquées ne portent pas une atteinte manifestement disproportionnée au droit au respect de la vie privée ; que, par suite, les dispositions des articles L. 851-4, L. 851-5 et L. 851-6 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

Document 9 : CE, Ord., 13 mai 2015, *Association de défense et d'assistance juridique des intérêts des supporters et autres*, n°389816, 389861, 389866, 389899.

Ordonnance du 13 mai 2015
Le juge des référés

Vu la procédure suivante :

1° Sous le n° 389816, par une requête et un nouveau mémoire, enregistrés les 28 avril et 11 mai 2015 au secrétariat du contentieux du Conseil d'Etat, l'association de défense et d'assistance juridique des intérêts des supporters (ADAJIS) demande au juge des référés du Conseil d'Etat, statuant sur le fondement de l'article L. 521-1 du code de justice administrative :

1°) à titre principal, d'ordonner la suspension de l'exécution de l'arrêté du 15 avril 2015 du ministre de l'intérieur portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « fichier STADE » ;

2°) à titre subsidiaire, d'ordonner la suspension de l'exécution de l'article 1er de cet arrêté en ce qu'il vise les manifestations sportives du club du Paris Saint-Germain et des rassemblements liés à ces manifestations se tenant à l'extérieur des départements relevant des compétences du préfet de police ainsi que de l'article 5 de cet arrêté en ce qu'il prévoit que les associations sportives, les sociétés sportives et les fédérations sportives agréées peuvent être destinataires des informations figurant au « fichier STADE » ;

3°) de mettre à la charge de l'Etat la somme de 2 500 euros au titre de l'article L. 761-1 du code de justice administrative.
Elle soutient que :
- la condition d'urgence est remplie dès lors que l'arrêté contesté porte une atteinte grave et immédiate au droit au respect de la vie privée, à raison des données collectées et des abus que ce traitement autorise ;
- il existe un doute sérieux quant à la légalité de l'arrêté contesté ;
- il est, en effet, entaché d'incompétence dès lors qu'il permet la création d'un traitement de données à caractère personnel ayant une double finalité de police administrative et de police judiciaire alors que seul le législateur pouvait créer et autoriser un tel traitement ;
- il autorise la collecte de données faisant apparaître directement et indirectement les origines raciales ou ethniques, les opinions politiques et l'appartenance syndicale des intéressés, qui ne peuvent être recueillies qu'en vertu d'un décret en Conseil d'Etat ;
- il méconnaît les dispositions de l'article 6 de la loi du 6 janvier 1978 qui prévoient que les données doivent être collectées pour des finalités déterminées, explicites et légitimes et être, au regard de ces finalités, adéquates, pertinentes et non excessives, de telle sorte que l'arrêté portant création du traitement doit être rédigé de façon précise et intelligible, que ce traitement ne peut s'étendre au-delà du ressort territorial de l'autorité désignée pour le mettre en œuvre, qu'il ne peut reposer sur une rupture d'égalité, qu'il ne peut servir de fondement à des mesures méconnaissant les droits fondamentaux, que ce traitement ne se justifie que dans la mesure où il n'existe pas déjà d'autres traitements permettant de poursuivre les mêmes finalités et que des garanties sont offertes quant à la conservation des données ;
- la transmission des données aux associations et sociétés sportives, qui n'ont pas de pouvoirs de police, méconnaît le droit d'information et le droit d'opposition, ne répond pas à des finalités légitimes et ne comporte pas de garanties concernant la conservation des données.
2° Sous le n° 389861, par une requête et un nouveau mémoire, enregistrés les 29 avril et 11 mai 2015 au secrétariat du contentieux du Conseil d'Etat, la Ligue des droits de l'homme demande au juge des référés du Conseil d'Etat, statuant sur le fondement de l'article L. 521-1 du code de justice administrative :

1°) à titre principal, d'ordonner la suspension de l'exécution de l'arrêté du 15 avril 2015 du ministre de l'intérieur portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « fichier STADE » ;

2°) à titre subsidiaire, d'ordonner la suspension de l'exécution de l'article 1er de cet arrêté en ce qu'il vise les manifestations sportives du club du Paris Saint-Germain et des rassemblements liés à ces manifestations se tenant à l'extérieur des départements relevant des compétences du préfet de police ainsi que de l'article 5 de cet arrêté en ce qu'il prévoit que les associations sportives, les sociétés sportives et les fédérations sportives agréées peuvent être destinataires des informations figurant au « fichier STADE » ;

3°) de mettre à la charge de l'Etat la somme de 2 000 euros au titre de l'article L. 761-1 du code de justice administrative.
Elle invoque les mêmes moyens que ceux présentés dans la requête n° 389816.
3° Sous le n° 389866, par une requête et un nouveau enregistrés les 29 avril et 11 mai 2015 au secrétariat du contentieux du Conseil d'Etat, l'association Lutte pour un Football Populaire demande au juge des référés du Conseil d'Etat, statuant sur le fondement de l'article L. 521-1 du code de justice administrative :

1°) à titre principal, d'ordonner la suspension de l'exécution de l'arrêté du 15 avril 2015 du ministre de l'intérieur portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « fichier STADE » ;

2°) à titre subsidiaire, d'ordonner la suspension de l'exécution de l'article 1er de cet arrêté en ce qu'il vise les manifestations sportives du club du Paris Saint-Germain et des rassemblements liés à ces manifestations se tenant à l'extérieur des départements relevant des compétences du préfet de police ainsi que de l'article 5 de cet arrêté en ce qu'il prévoit que les associations sportives, les sociétés sportives et les fédérations sportives agréées peuvent être destinataires des informations figurant au « fichier STADE » ;

3°) de mettre à la charge de l'Etat la somme de 1 500 euros au titre de l'article L. 761-1 du code de justice administrative.
Elle invoque les mêmes moyens que ceux présentés dans la requête n° 389816.
4° Sous le n° 389899, par une requête et un nouveau mémoire, enregistrés les 1er mai et 11 mai 2015 au secrétariat du contentieux du Conseil d'Etat, l'Association Nationale des Supporters demande au juge des référés du Conseil d'Etat, statuant sur le fondement de l'article L. 521-1 du code de justice administrative :

1°) à titre principal, d'ordonner la suspension de l'exécution de l'arrêté du 15 avril 2015 du ministre de l'intérieur portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « fichier STADE » ;

2°) à titre subsidiaire, d'ordonner la suspension de l'exécution de l'article 1er de cet arrêté en ce qu'il vise les manifestations sportives du club du Paris Saint-Germain et des rassemblements liés à ces manifestations se tenant à l'extérieur des départements relevant des

compétences de police de Monsieur le préfet de Police ainsi que de l'article 5 de cet arrêté en ce qu'il prévoit que les associations sportives, les sociétés sportives et les fédérations sportives agréées peuvent être destinataires des informations figurant au « fichier STADE » ;

3°) de mettre à la charge de l'Etat la somme de 2 000 euros au titre de l'article L. 761-1 du code de justice administrative.
Elle invoque les mêmes moyens que ceux présentés dans la requête n° 389816.
Vu l'arrêté dont la suspension de l'exécution est demandée ;
Vu la copie des requêtes à fin d'annulation de cet arrêté ;
Par un mémoire en intervention, enregistré le 11 mai 2015, l'association La Voix de l'Enfant demande au juge des référés du Conseil d'Etat de faire droit aux conclusions des requérantes et de mettre à la charge de l'Etat la somme de 3 000 euros au titre de l'article L. 761-1 du code de justice administrative.
Elle soutient que :
- elle a intérêt à intervenir ;
- l'urgence est caractérisée par le fait qu'une association sportive pourrait connaître les antécédents judiciaires de tout supporter sans être soumise à une quelconque obligation quant à la confidentialité de ces informations ;
- que la décision créant le traitement informatisé litigieux ne pouvait être prise que par décret en Conseil d'Etat ;
- que l'arrêté méconnaît le droit au respect de la vie privée et l'interdiction de rapprocher les données issues de traitements automatisés différents.
Par un mémoire en défense et un nouveau mémoire, enregistrés les 7 et 11 mai 2015, le ministre de l'intérieur conclut au rejet des requêtes. Il soutient que la requête de l'ADAJIS est irrecevable, que l'association La Voix de l'Enfant n'est pas recevable à intervenir et que les moyens soulevés par les associations requérantes et intervenante ne sont pas fondés.
Vu les autres pièces des dossiers ;
Vu :
- la loi n° 78-17 du 6 janvier 1978 ;
- le code de justice administrative ;
Après avoir convoqué à une audience publique, d'une part, l'association de défense et d'assistance juridique des intérêts des supporters, la Ligue des droits de l'homme, l'Association Lutte pour un Football Populaire, l'Association Nationale des Supporters, l'association La Voix de l'Enfant et, d'autre part, le ministre de l'intérieur ;
Vu le procès-verbal de l'audience publique du 12 mai à 14 heures au cours de laquelle ont été entendus :
- Me Lécuyer, avocat au Conseil d'Etat et à la Cour de cassation, avocat de l'association de défense et d'assistance juridique des intérêts des supporters, de la Ligue des droits de l'homme, de l'association Lutte pour un Football Populaire et de l'Association Nationale des Supporters ;
- les représentants de l'association de défense et d'assistance juridique des intérêts des supporters ;
- les représentants de la Ligue des droits de l'homme ;
- les représentants de l'association Lutte pour un Football Populaire ;
- les représentants de l'Association Nationale des Supporters ;
- Me Colin, avocat au Conseil d'Etat et à la Cour de cassation, avocat de l'association La

Voix de l'Enfant ;
- les représentants de l'association La Voix de l'Enfant ;
- les représentants du ministre de l'intérieur ;
et à l'issue de laquelle le juge des référés a clos l'instruction ;

1. Considérant que les requêtes de l'Association de défense et d'assistance juridique des intérêts des supporters, de la Ligue des droits de l'homme, de l'association Lutte pour un Football Populaire et de l'Association Nationale des Supporters sont dirigées contre le même arrêté ; qu'il y a lieu de les joindre pour statuer par une seule ordonnance ;

2. Considérant que l'association La Voix de l'Enfant a intérêt à la suspension de l'arrêté contesté ; que son intervention est, par suite, recevable ;

3. Considérant qu'aux termes du premier alinéa de l'article L. 521-1 du code de justice administrative : « *Quand une décision administrative, même de rejet, fait l'objet d'une requête en annulation ou en réformation, le juge des référés, saisi d'une demande en ce sens, peut ordonner la suspension de l'exécution de cette décision, ou de certains de ses effets, lorsque l'urgence le justifie et qu'il est fait état d'un moyen propre à créer, en l'état de l'instruction, un doute sérieux quant à la légalité de la décision* » ;

4. Considérant que, par l'arrêté dont les associations requérantes demandent la suspension de l'exécution, le ministre de l'intérieur a autorisé le préfet de police à mettre en œuvre un traitement automatisé de données à caractère personnel visant à prévenir les troubles à l'ordre public, les atteintes à la sécurité des personnes et des biens ainsi que les infractions susceptibles d'être commises à l'occasion de manifestations sportives et de rassemblements en lien avec ces manifestations ; que les données collectées, qui ne peuvent être enregistrées dans le traitement que si elles sont nécessaires à la poursuite de cette finalité, peuvent concerner toute personne « se prévalant de la qualité de supporter d'une équipe ou se comportant comme tel », qu'elle soit majeure ou mineure âgée d'au moins treize ans ; que les données pouvant être enregistrées, outre le motif de leur enregistrement et l'identité de la personne, incluent notamment la profession de celle-ci et son adresse, ses « signes physiques particuliers et objectifs, photographies », ses « activités publiques, comportements et déplacements, blogs et réseaux sociaux, en lien avec les groupes de supporters d'appartenance », les « personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé », ainsi que des données issues de plusieurs autres traitements automatisés mis en œuvre par le ministère de l'intérieur ; que tout ou partie de ces données peut être transmis, non seulement à des autorités administratives et judiciaires, mais aussi aux « associations et sociétés sportives » ;

5. Considérant qu'aux termes de l'article 6 de la loi du 6 janvier 1978 : « *Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : / 1° Les données sont collectées et traitées de manière loyale et licite ; / 2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités […] ; 3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ; […]* » ;

6. Considérant que les associations requérantes soutiennent que le traitement automatisé que l'arrêté a pour objet d'autoriser, compte tenu du caractère général et indéterminé des finalités qui lui sont imparties, ne définit avec une précision suffisante ni les personnes concernées par ce traitement, ni les catégories de données qui peuvent être enregistrées, dont certaines pourraient d'ailleurs relever du I de l'article 8 de la loi du 6 janvier 1978 ; que le moyen tiré de ce que le traitement ainsi défini ne porte pas sur des données adéquates, pertinentes et non excessives au sens de l'article 6 de la même loi est de nature à créer, en l'état de l'instruction et en dépit des explications données à l'audience par les représentants du ministre de l'intérieur, un doute sérieux quant à la légalité de l'arrêté du 15 avril 2015 ;

7. Considérant que l'urgence justifie la suspension de l'exécution d'un acte administratif lorsque celui-ci porte atteinte de manière suffisamment grave et immédiate à un intérêt public, à la situation du requérant ou aux intérêts qu'il entend défendre ; qu'en l'espèce, l'arrêté porte une atteinte grave et immédiate au droit au respect de la vie privée des personnes concernées, tant par la nature des données collectées et traitées et leur possible utilisation pour l'exercice des compétences dévolues à l'autorité préfectorale par l'article L. 332-16 du code du sport, que par la transmission des données collectées aux clubs sportifs sans garantie suffisante quant à leur utilisation par ceux-ci ; que dès lors les effets de l'acte contesté sont de nature à caractériser une urgence justifiant que, sans attendre le jugement de la requête au fond, l'exécution de la décision soit suspendue ;

8. Considérant qu'il y a lieu, dans les circonstances de l'espèce, de mettre à la charge de l'Etat une somme de 1 000 euros à verser à chacune des associations requérantes au titre de l'article L. 761-1 du code de justice administrative ; qu'en revanche les dispositions de ce même article font obstacle à ce qu'une somme soit versée à ce titre à l'association La Voix de l'Enfant qui n'a pas, dans la présente instance, la qualité de partie ;

O R D O N N E :

Article 1er : L'intervention de l'association La Voix de l'Enfant est admise.

Article 2 : Jusqu'à ce que le Conseil d'Etat, statuant au contentieux, ait statué sur sa légalité, l'exécution de l'arrêté du 15 avril 2015 du ministre de l'intérieur portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « fichier STADE » est suspendue.

Article 3 : L'Etat versera, au titre de l'article L. 761-1 du code de justice administrative, une somme de 1 000 euros à l'Association de défense et d'assistance juridique des intérêts des supporters, une somme de 1 000 euros à la Ligue des droits de l'homme, une somme de 1 000 euros à l'Association Lutte pour un Football Populaire et une somme de 1 000 euros à l'Association Nationale des Supporters.

Article 4 : Les conclusions présentées par l'association La Voix de l'Enfant au titre de l'article L. 761-1 du code de justice administrative sont rejetées.

Article 5 : La présente ordonnance sera notifiée à l'Association de défense et d'assistance juridique des intérêts des supporters, à la Ligue des droits de l'homme, à l'Association Lutte pour un Football Populaire, à l'Association Nationale des Supporters, à l'association la Voix de l'Enfant et au ministre de l'intérieur.

<u>Document 10</u> : L. PEILLON, « Ménard aurait ses fiches ethniques ''seul'' et pour ''quelques écoles'' », *Liberation*, 7 mai 2015.

Devant le tribunal administratif, l'avocate du maire de Béziers a relativisé le chiffre de 64 % d'élèves musulmans. Au risque de ridiculiser son auteur.

Robert Ménard fait profil bas, quitte à minorer largement la pertinence de ses statistiques ethniques. Sur France 2, lundi, le maire de Béziers avait avoué s'être livré – sur la base des prénoms – à un comptage des élèves musulmans, estimant qu'ils représentaient deux tiers des écoles biterroises. *«Dans ma ville, il y a 64,6 % des enfants qui sont musulmans dans les écoles primaires et maternelles»*, expliquait-il alors.
Convoqué jeudi après-midi devant le tribunal administratif de Montpellier, suite à une requête du CRI (Coordination contre le racisme et l'islamophobie), Robert Ménard était représenté par son avocate, Me Raphaële Hiault-Spitzer. Or, selon *Midi Libre*, le conseil du maire de Béziers, qui a réaffirmé que *«ces fichiers n'existent pas»*, a expliqué que le maire *«seul […], a pris une liste de quelques écoles»* et *«a fait une analyse à titre de réflexion»*. Une version confirmée à *Libération* par l'avocat du CRI, Me Gilles Devers. Pour ce dernier, cependant, cette explication ne change rien. *«Ce n'est pas tant l'existence du fichier qui importe et qui est contraire à la loi, mais le traitement des données issues de ce fichier. Et qu'il l'ait fait sur quelques écoles ne change pas grand-chose.»*
Si cette version est vraie, elle relativise en tout cas largement le sens du chiffre de 64 % livré par Robert Ménard, cette donnée étant loin de concerner l'ensemble des 6600 élèves de la ville.

Saisi en référé, le tribunal administratif de Montpellier rendra une décision lundi. Le CRI demande au juge administratif de contraindre la commune de Béziers à cesser tout acte de collecte, d'enregistrement, d'organisation, de consultation et d'utilisation de traitement des informations sur la religion des élèves scolarisés sur sa commune.