



Décision n° 2017 - 670 QPC

Article 230-8 du code de procédure pénale

*Effacement anticipé des données à caractère personnel
inscrites dans un fichier de traitement d'antécédents
judiciaires*

Dossier documentaire

Source : services du Conseil constitutionnel © 2017

Sommaire

I. Dispositions législatives.....	4
II. Constitutionnalité de la disposition contestée	52

Table des matières

I. Dispositions législatives.....	4
A. Dispositions contestées	4
1. Code de procédure pénale	4
- Article 230-8	4
B. Évolution des dispositions contestées	5
1. Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure	5
- Article 11	5
2. Ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure	6
- Article 1 ^{er}	6
- Article 3	6
- Article 19	6
- Annexe	8
- Extrait de la table de concordance	8
- Article 230-8 tel que modifié par l'ordonnance n° 2012-351	9
3. Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.....	10
- Article 68	10
- Article 230-8 tel que modifié par la loi n° 2016-731	11
C. Autres dispositions	11
1. Code de sécurité intérieure.....	11
- Article L. 114-1.....	11
- Article L. 234-1.....	12
- Article L. 234-2.....	12
- Article L. 234-3.....	12
2. Code de procédure pénale	12
- Article 230-6	12
- Article 230-7	13
- Article 230-9	13
- Article 230-10	13
- Article 706-25-12.....	14
- Article 706-53-10.....	14
- Article 706-54	14
- Article R. 40-23	15
- Article R. 40-24	16
- Article R. 40-25	16
- Article R. 40-26	16
- Article R. 40-27	18
- Article R. 40-28	20
- Article R. 40-29	21
- Article R. 40-29-1	22
- Article R. 40-31	22
- Article R. 40-31-1	22
- Article R. 40-32	23
- Article R. 40-33	23
- Article R. 40-34	23
3. Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité	23
- Article 17-1	23

D. Application des dispositions contestées	24
1. Jurisprudence	24
a. Jurisprudence de la CEDH	24
- CEDH, 26 mars 1987, <i>Leander c. Suède</i> , n° 9248/81	24
- CEDH, 16 février 2000, <i>Amann c. Suisse</i> , n° 27798/ 95	24
- CEDH, 4 décembre 2008, <i>S. et Marper c. Royaume-Uni</i> , n° 30562/04 et 30566/04.....	26
- CEDH, 17 décembre 2009, <i>M. B. c. France</i> , n° 22115/06.....	36
- CEDH, 18 avril 2013, <i>M. K. c. France</i> , n° 19522/09.....	39
- CEDH, 18 septembre 2014, <i>Brunet c/ France</i> , n° 21010/10	42
- CEDH, 22 juin 2017, <i>Aycaguer c. France</i> , n° 8806/2	44
b. Jurisprudence administrative	47
- CE, 17 juillet 2013, n° 359417.....	47
- CE, 11 avril 2014, n° 360759.....	48
- CE, avis 30 mars 2016, n° 395119.....	49
c. Jurisprudence judiciaire.....	50
- Cass. crim. 9 avril 2008, n° 07-85972.....	50
II. Constitutionnalité de la disposition contestée	52
A. Normes de référence	52
Déclaration des droits de l’homme et du citoyen de 1789	52
- Article 2	52
B. Jurisprudence du Conseil constitutionnel	52
Sur l’atteinte au droit au respect de la vie privée	52
- Décision n° 99-416 DC du 23 juillet 1999 - Loi portant création d'une couverture maladie universelle.....	52
- Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure.....	53
- Décision n° 2010-25 QPC du 16 septembre 2010 - M. Jean-Victor C. (<i>Fichier empreintes génétiques</i>).....	55
- Décision n° 2011-625 DC du 10 mars 2011 - Loi d'orientation et de programmation pour la performance de la sécurité intérieure.....	56
- Décision n° 2012-652 DC du 22 mars 2012 - Loi relative à la protection de l'identité	57
- Décision n° 2014-690 DC du 13 mars 2014 - Loi relative à la consommation	58
- Décision n° 2015-727 DC du 21 janvier 2016 - Loi de modernisation de notre système de santé...59	
- Décision n° 2016-591 QPC du 21 octobre 2016 - Mme Helen S. (<i>Registre public des trusts</i>)	60
- Décision n° 2016-744 DC du 29 décembre 2016 - Loi de finances pour 2017	61
- Décision n° 2016-745 DC du 26 janvier 2017 - Loi relative à l'égalité et à la citoyenneté	61
- Décision n° 2017-637 QPC du 16 juin 2017 - Association nationale des supporters (<i>Refus d'accès à une enceinte sportive et fichier d'exclusion</i>).....	62

I. Dispositions législatives

A. Dispositions contestées

1. Code de procédure pénale

- Article 230-8

Modifié par loi n°2016-731 du 3 juin 2016 - art. 68

Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquittement ou de relaxe devenue définitive, il en avise la personne concernée. Les décisions de non-lieu et de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé.

Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la durée de conservation des données personnelles.

Les décisions du procureur de la République en matière d'effacement ou de rectification des données personnelles sont susceptibles de recours devant le président de la chambre de l'instruction.

Le procureur de la République dispose pour l'exercice de ses fonctions d'un accès direct aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6.

B. Évolution des dispositions contestées

1. Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

- Article 11

I. — Le chapitre unique du titre IV du livre Ier du code de procédure pénale devient le chapitre Ier du même titre et, après l'article 230-5, il est ajouté un chapitre II ainsi rédigé :

« Chapitre II

« Des fichiers de police judiciaire

« Section 1

« Des fichiers d'antécédents

« Art. 230-6.-Afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, les services de la police nationale et de la gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel recueillies :

« 1° Au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant :

« a) Un trouble à la sécurité ou à la tranquillité publiques ;

« b) Une atteinte aux personnes, aux biens ou à l'autorité de l'Etat ;

« 2° Au cours des procédures de recherche des causes de la mort mentionnées à l'article 74 ou de recherche des causes d'une disparition mentionnées à l'article 74-1.

« Ces traitements ont également pour objet l'exploitation des informations recueillies à des fins de recherches statistiques.

« Art. 230-7.-Les traitements mentionnés à l'article 230-6 peuvent contenir des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées au 1° du même article 230-6.

« Ils peuvent également contenir des informations sur les victimes de ces infractions. Ces dernières peuvent toutefois s'opposer à ce que les données à caractère personnel les concernant soient conservées dans le fichier dès lors que l'auteur des faits a été définitivement condamné.

« Ils peuvent en outre contenir des informations sur les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort mentionnée à l'article 74 ou d'une enquête ou d'une instruction pour recherche des causes d'une disparition mentionnée à l'article 74-1. Les données personnelles concernant ces dernières sont effacées dès lors que l'enquête a permis de retrouver la personne disparue ou d'écarter toute suspicion de crime ou délit.

« **Art. 230-8.-Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. En cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquiescement ou de relaxe devenue définitive, il en avise la personne concernée. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Les autres décisions de classement sans suite font l'objet d'une mention. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues à l'[article 17-1 de la loi n° 95-73 du 21 janvier 1995](#) d'orientation et de programmation relative à la sécurité.**

« Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la durée de conservation des données personnelles.

« Le procureur de la République dispose pour l'exercice de ses fonctions d'un accès direct aux

traitements automatisés de données à caractère personnel mentionnés à l'article 230-6.

« Art. 230-9.-Un magistrat, chargé de suivre la mise en œuvre et la mise à jour des traitements automatisés de données à caractère personnel mentionnés à l'article 230-6 et désigné à cet effet par le ministre de la justice, concourt à l'application de l'article 230-8.

« Ce magistrat peut agir d'office ou sur requête des particuliers. Il dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles dans les traitements mentionnés au premier alinéa du présent article que le procureur de la République. Lorsque la personne concernée le demande, la rectification pour requalification judiciaire est de droit. Il se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois.

« Il dispose, pour l'exercice de ses fonctions, d'un accès direct à ces traitements automatisés.

« Art. 230-10.-Les personnels spécialement habilités des services de la police et de la gendarmerie nationales désignés à cet effet ainsi que les personnels spécialement habilités de l'Etat investis par la loi d'attributions de police judiciaire, notamment les agents des douanes, peuvent accéder aux informations, y compris nominatives, figurant dans les traitements de données personnelles prévus par la présente section et détenus par chacun de ces services.L'habilitation précise la nature des données auxquelles elle autorise l'accès.L'accès, par tous moyens techniques mobiles, aux informations figurant dans les traitements de données personnelles prévus par la présente section est ouvert aux seuls personnels de la police et de la gendarmerie nationales et des douanes.

« L'accès aux informations mentionnées au premier alinéa est également ouvert :

« 1° Aux magistrats du parquet ;

« 2° Aux magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis.

« Art. 230-11.-Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application de la présente section. Il précise notamment la liste des contraventions mentionnées à l'article 230-6, la durée de conservation des informations enregistrées, les modalités d'habilitation des personnes mentionnées à l'article 230-10 ainsi que, le cas échéant, les conditions dans lesquelles les personnes intéressées peuvent exercer leur droit d'accès.

2. Ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure

[Ordonnance ratifiée par l'article 24 de la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme](#)

- Article 1^{er}

Les dispositions annexées à la présente ordonnance constituent la partie législative du code de la sécurité intérieure.

- Article 3

Les références à des dispositions abrogées par la présente ordonnance sont remplacées par des références aux dispositions correspondantes du code de la sécurité intérieure.

- Article 19

Sont abrogés, sous réserve des dispositions de l'article 20 :

1° Les articles L. 412-46, L. 412-48, L. 412-49 (à l'exception de la dernière phrase), L. 412-49-1, L. 412-51 à L. 412-54 et L. 441-2 du code des communes ;

2° Les articles L. 132-2 à L. 132-4, L. 133-1, L. 411-3 et L. 411-4 du code des communes de la Nouvelle-Calédonie ;

3° L'article L. 127-1 du code de la construction et de l'habitation ;

4° Les III et IV de l'article L. 2332-1, les articles L. 2332-1-1, L. 2336-2 à L. 2336-6, L. 2337-2 à L. 2337-5, L. 2338-1, L. 2339-6 à L. 2339-8 et L. 4231-5 du code de la défense ;

- 5° Les articles L. 1424-8-2 à L. 1424-8-8, L. 2211-2 à L. 2211-5, L. 2212-2-1, L. 2212-6 à L. 2212-10, L. 2213-16, L. 2213-18 à L. 2213-19-1, L. 2215-2, L. 2215-6, L. 2215-7, L. 2216-3, L. 2512-14-1, L. 2512-14-2, L. 2512-15, L. 2512-16-1, les III et IV de l'article L. 2573-18, l'article L. 5211-60 et l'article L. 6161-37 du code général des collectivités territoriales ;
- 6° Les articles L. 5261-1 à L. 5261-3 du code des transports ;
- 7° Les articles L. 3142-109 à L. 3142-111, L. 3142-113 et L. 3142-114 du code du travail ;
- 8° La loi du 21 mai 1836 portant prohibition des loteries ;
- 9° La loi du 15 juin 1907 relative aux casinos ;
- 10° Le décret-loi du 23 octobre 1935 portant réglementation des mesures relatives au renforcement du maintien de l'ordre public ;
- 11° La loi du 10 janvier 1936 sur les groupes de combat et milices privées ;
- 12° La loi n° 47-2384 du 27 décembre 1947 portant réorganisation des compagnies républicaines de sécurité ;
- 13° Le premier alinéa de l'article 2 de la loi n° 48-1504 du 28 septembre 1948 relative au statut spécial des personnels de police ;
- 14° La loi n° 66-383 du 16 juin 1966 relative aux opérations de déminage poursuivies par l'Etat ;
- 15° La loi n° 66-492 du 9 juillet 1966 portant organisation de la police nationale ;
- 16° Les deuxième à sixième alinéas du III, le IV et le V de l'article 34 de la loi n° 82-213 du 2 mars 1982 relative aux droits et libertés des communes, des départements et des régions ;
- 17° La loi n° 83-628 du 12 juillet 1983 relative aux jeux de hasard ;
- 18° Les articles 1er à 11,11-5 à 35 de la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité ;
- 19° La loi n° 85-835 du 7 août 1985 relative à la modernisation de la police nationale ;
- 20° La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques ;
- 21° Les articles 1er, 3,10,10-1,10-2, l'article 17-1 à l'exception de son troisième alinéa, l'article 18, le premier alinéa de l'article 19, les articles 23,23-1 et 25-1, les 2° à 6° de l'article 31 et les I et I bis de l'article 36 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité ;**
- 22° Les articles 1er à 1-4,1-6 à 6,9 et 26 de la loi n° 96-370 du 3 mai 1996 relative au développement du volontariat dans les corps de sapeurs-pompiers ;
- 23° La loi n° 2000-646 du 10 juillet 2000 relative à la sécurité du dépôt et de la collecte de fonds par les entreprises privées ;
- 24° Les I, II, III et VI de l'article 58 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ;
- 25° Les articles 5 et 8 de la loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure ;
- 26° Les articles 4 à 6,24 et 26 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure ;
- 27° Les articles 1er, 2,4, les I à III de l'article 6, les articles 7 à 43,45,47 à 70,72,74 à 93,95 à 103 de la loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile ;
- 28° Les articles 7 et 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers ;
- 29° Les I et III de l'article 43 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure ;
- 30° Les articles 3 et 4 de l'ordonnance n° 92-1145 du 12 octobre 1992 portant extension et adaptation dans les territoires d'outre-mer des dispositions législatives relatives au secret des correspondances émises par la voie des télécommunications ;
- 31° L'article 14 de l'ordonnance n° 2002-1450 du 12 décembre 2002 relative à la modernisation du régime communal, à la coopération intercommunale, aux conditions d'exercice des mandats locaux à Mayotte et modifiant le code général des collectivités territoriales (partie législative) ;
- 32° Les articles 71 et 72 de l'ordonnance n° 2005-10 du 4 janvier 2005 portant statut général des fonctionnaires des communes et des groupements de communes de la Polynésie française ainsi que de leurs établissements publics administratifs ;
- 33° Les articles 1er à 22 et 31 de l'ordonnance n° 2006-172 du 15 février 2006 portant actualisation et adaptation du droit applicable en matière de sécurité civile en Nouvelle-Calédonie ;
- 34° Les articles 1er à 21,31 et 32 de l'ordonnance n° 2006-173 du 15 février 2006 portant actualisation et adaptation du droit applicable en matière de sécurité civile en Polynésie française.

- Annexe

Article L. 114-1

Les décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées.

Article L. 234-1

Un décret en Conseil d'Etat fixe la liste des enquêtes administratives mentionnées à l'article L. 114-1 qui donnent lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'**article 230-6 du code de procédure pénale**, y compris pour les données portant sur des procédures judiciaires en cours, dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la Nation. Il détermine les conditions dans lesquelles les personnes intéressées sont informées de cette consultation.

Article L. 234-1

Un décret en Conseil d'Etat fixe la liste des enquêtes administratives mentionnées à l'article L. 114-1 qui donnent lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'**article 230-6 du code de procédure pénale**, y compris pour les données portant sur des procédures judiciaires en cours, dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la Nation. Il détermine les conditions dans lesquelles les personnes intéressées sont informées de cette consultation.

- Extrait de la table de concordance

Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité	art. 1 ^{er}	L. 111-1
	art. 3	L. 111-2
	art. 10, I	L. 251-1
	art. 10, II, al. 1 à 12 ecqc les actes de terrorisme	L. 223-1
	art. 10, II, al. 1 à 12 sauf ecqc les actes de terrorisme	L. 251-2
	art. 10, II, al. 13 et 14	L. 251-3
	art. 10, III, al. 1 et 5	L. 252-1
	art. 10, III, al. 2	L. 252-2
	art. 10, III, al. 3	L. 252-3
	art. 10, III, al. 4, 6 et 17	L. 252-4
	art. 10, III, al. 7	L. 253-1
	art. 10, III, al. 8	L. 253-2
	art. 10, III, al. 9 à 15	L. 253-3
	art. 10, III, al. 16	L. 253-4
	art. 10, III bis ecqc les actes de	L. 223-4

	terrorisme	
	art. 10, III bis sauf ecqc les actes de terrorisme	L. 252-6
	art. 10, IV	L. 252-5
	art. 10, V	L. 253-5
	art. 10, VI	L. 254-1
	art. 10, VI bis	L. 251-7
	art. 10, VII	L. 255-1
	art. 10-1, I	L. 223-2
	art. 10-1, II	L. 223-3
	art. 10-1, III ecqc les actes de terrorisme	L. 223-5
	art. 10-1, III sauf ecqc les actes de terrorisme	L. 252-7
	art. 10-1, IV	L. 223-6
	art. 10-1, V	L. 223-7
	art. 10-1, VI	L. 223-8
	art. 10-1, VII	L. 223-9
	art. 10-2, al. 1 à 3	L. 251-5
	art. 10-2, al. 4 à 11	L. 251-6
	art. 17-1, al. 1	L. 114-1
	art. 17-1, al. 2	L. 234-1
	art. 17-1, al. 4	L. 234-2
	art. 17-1, al. 5	L. 234-3
	art. 18, I	L. 211-13
	art. 18, II	L. 211-14
	art. 19, al. 1	L. 411-2
	art. 23	L. 211-11
	art. 23-1, al. 1 et 2	L. 211-5
	art. 23-1, al. 3	L. 211-6
	art. 23-1, al. 4 et 5	L. 211-7
	art. 23-1, al. 6	L. 211-15
	art. 23-1, al. 8	L. 211-8
	art. 25-1	L. 214-2
	art. 36, I, al. 1 et 3	L. 411-5
	art. 36, I bis	L. 411-6

- **Article 230-8 tel que modifié par l'ordonnance n° 2012-351**

Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification

dans un délai d'un mois. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquittement ou de relaxe devenue définitive, il en avise la personne concernée. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Les autres décisions de classement sans suite font l'objet d'une mention. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues **aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure** et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la durée de conservation des données personnelles.

Le procureur de la République dispose pour l'exercice de ses fonctions d'un accès direct aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6.

3. Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale

- Article 68

La section 1 du chapitre II du titre IV du livre Ier du même code est ainsi modifiée :

1° L'article 230-8 est ainsi modifié :

a) Le premier alinéa est ainsi modifié :

- à la quatrième phrase, les mots : « pour des raisons liées à la finalité du fichier » sont supprimés ;

- les sixième et avant-dernière phrases sont remplacées par une phrase ainsi rédigée :

« Les décisions de non-lieu et de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. » ;

- est ajoutée une phrase ainsi rédigée :

« Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé. » ;

b) Après le deuxième alinéa, il est inséré un alinéa ainsi rédigé :

« Les décisions du procureur de la République en matière d'effacement ou de rectification des données personnelles sont susceptibles de recours devant le président de la chambre de l'instruction. » ;

2° L'article 230-9 est complété par un alinéa ainsi rédigé :

« Les décisions de ce magistrat en matière d'effacement ou de rectification des données personnelles sont susceptibles de recours devant le président de la chambre de l'instruction de la cour d'appel de Paris. » ;

3° La seconde phrase de l'article 230-11 est complétée par les mots : « et contester les décisions prises par le procureur de la République ou le magistrat mentionné à l'article 230-9 ».

- **Article 230-8 tel que modifié par la loi n° 2016-731**

Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. En cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien ~~pour des raisons liées à la finalité du fichier~~, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquiescement ou de relaxe devenue définitive, il en avise la personne concernée. ~~Les décisions de non lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Les autres décisions de classement sans suite font l'objet d'une mention.~~ **Les décisions de non-lieu et de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles.** Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. **Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé.**

Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la durée de conservation des données personnelles.

Les décisions du procureur de la République en matière d'effacement ou de rectification des données personnelles sont susceptibles de recours devant le président de la chambre de l'instruction.

Le procureur de la République dispose pour l'exercice de ses fonctions d'un accès direct aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6.

C. Autres dispositions

1. Code de sécurité intérieure

- **Article L. 114-1**

Créé par ordonnance n°2012-351 du 12 mars 2012 - Annexe, v. init.

Les décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées.

- **Article L. 234-1**

Créé par Ordonnance n°2012-351 du 12 mars 2012 - Annexe, v. init.

Un décret en Conseil d'Etat fixe la liste des enquêtes administratives mentionnées à l'article L. 114-1 qui donnent lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 230-6 du code de procédure pénale, y compris pour les données portant sur des procédures judiciaires en cours, dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la Nation. Il détermine les conditions dans lesquelles les personnes intéressées sont informées de cette consultation.

- **Article L. 234-2**

Modifié par loi n°2015-912 du 24 juillet 2015 - art. 21 (V)

La consultation prévue à l'article L. 234-1 est faite par des agents individuellement désignés et spécialement habilités :

1° De la police et de la gendarmerie nationales ;

2° Dans des conditions fixées par le décret en Conseil d'Etat mentionné à l'article L. 234-1, des services spécialisés de renseignement mentionnés à l'article L. 811-2.

Dans des conditions déterminées par décret en Conseil d'Etat, elle peut également être effectuée par des personnels investis de missions de police administrative désignés selon les mêmes procédures.

NOTA :

Conformément à l'article 26 de la loi n° 2015-912 du 24 juillet 2015, à l'exception des articles 3, 4, 9, 16 à 20 et 22 et sous réserve des II à IV dudit article, la loi susmentionnée entre en vigueur au lendemain de la publication au Journal officiel du décret nommant le président de la Commission nationale de contrôle des techniques de renseignement.

- **Article L. 234-3**

Modifié par loi n°2013-1168 du 18 décembre 2013 - art. 19

La consultation des traitements automatisés de données personnelles mentionnés à l'article 230-6 du code de procédure pénale peut également être effectuée, y compris pour des données portant sur des procédures judiciaires en cours, pour l'exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, ainsi qu'au titre des mesures de protection ou de défense prises dans les secteurs de sécurité des installations prioritaires de défense mentionnés à l'article L. 1321-2 du code de la défense. Cette consultation est effectuée par des agents individuellement désignés et spécialement habilités de la police et de la gendarmerie nationales ainsi que, dans la limite de leurs attributions et dans des conditions fixées par décret en Conseil d'Etat, des services de renseignement désignés par le ministre de la défense, aux fins de protection de la sécurité de leurs personnels.

2. Code de procédure pénale

- **Article 230-6**

Créé par loi n°2011-267 du 14 mars 2011 - art. 11

Afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, les services de la police nationale et de la gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel recueillies :

1° Au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant :

a) Un trouble à la sécurité ou à la tranquillité publiques ;

b) Une atteinte aux personnes, aux biens ou à l'autorité de l'Etat ;

2° Au cours des procédures de recherche des causes de la mort mentionnées à l'article 74 ou de recherche des causes d'une disparition mentionnées à l'article 74-1.

Ces traitements ont également pour objet l'exploitation des informations recueillies à des fins de recherches statistiques.

- **Article 230-7**

Créé par loi n°2011-267 du 14 mars 2011 - art. 11

Les traitements mentionnés à l'article 230-6 peuvent contenir des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées au 1° du même article 230-6.

Ils peuvent également contenir des informations sur les victimes de ces infractions. Ces dernières peuvent toutefois s'opposer à ce que les données à caractère personnel les concernant soient conservées dans le fichier dès lors que l'auteur des faits a été définitivement condamné.

Ils peuvent en outre contenir des informations sur les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort mentionnée à l'article 74 ou d'une enquête ou d'une instruction pour recherche des causes d'une disparition mentionnée à l'article 74-1. Les données personnelles concernant ces dernières sont effacées dès lors que l'enquête a permis de retrouver la personne disparue ou d'écartier toute suspicion de crime ou délit.

- **Article 230-9**

Modifié par loi n°2016-731 du 3 juin 2016 - art. 68

Un magistrat, chargé de suivre la mise en œuvre et la mise à jour des traitements automatisés de données à caractère personnel mentionnés à l'article 230-6 et désigné à cet effet par le ministre de la justice, concourt à l'application de l'article 230-8.

Ce magistrat peut agir d'office ou sur requête des particuliers. Il dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles dans les traitements mentionnés au premier alinéa du présent article que le procureur de la République. Lorsque la personne concernée le demande, la rectification pour requalification judiciaire est de droit. Il se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois.

Il dispose, pour l'exercice de ses fonctions, d'un accès direct à ces traitements automatisés.

Les décisions de ce magistrat en matière d'effacement ou de rectification des données personnelles sont susceptibles de recours devant le président de la chambre de l'instruction de la cour d'appel de Paris.

- **Article 230-10**

Créé par loi n°2011-267 du 14 mars 2011 - art. 11

Les personnels spécialement habilités des services de la police et de la gendarmerie nationales désignés à cet effet ainsi que les personnels spécialement habilités de l'Etat investis par la loi d'attributions de police judiciaire, notamment les agents des douanes, peuvent accéder aux informations, y compris nominatives, figurant dans les traitements de données personnelles prévus par la présente section et détenus par chacun de ces services. L'habilitation précise la nature des données auxquelles elle autorise l'accès. L'accès, par tous moyens techniques mobiles, aux informations figurant dans les traitements de données personnelles prévus par la présente section est ouvert aux seuls personnels de la police et de la gendarmerie nationales et des douanes.

L'accès aux informations mentionnées au premier alinéa est également ouvert :

1° Aux magistrats du parquet ;

2° Aux magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis.

Livre IV : De quelques procédures particulières

Titre XV : De la poursuite, de l'instruction et du jugement des actes de terrorisme

- **Article 706-25-12**

Créé par loi n°2015-912 du 24 juillet 2015 - art. 19 (V)

Toute personne dont l'identité est inscrite dans le fichier peut demander au procureur de la République de rectifier ou d'ordonner l'effacement des informations la concernant si les informations ne sont pas exactes ou si leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier, au regard de la nature de l'infraction, de l'âge de la personne lors de sa commission, du temps écoulé depuis lors et de la personnalité actuelle de l'intéressé.

La même demande peut être faite au juge d'instruction lorsque l'inscription a été prise sur le fondement du 5° de l'article 706-25-4.

La demande d'effacement est irrecevable tant que les mentions sont relatives à une procédure judiciaire en cours, sauf dans l'hypothèse d'une inscription sur le fondement du même 5°.

Si le procureur de la République ou le juge d'instruction n'ordonne pas la rectification ou l'effacement, la personne peut saisir à cette fin le juge des libertés et de la détention, dont la décision peut être contestée devant le président de la chambre de l'instruction.

Avant de statuer sur la demande de rectification ou d'effacement, le procureur de la République, le juge des libertés et de la détention, le juge d'instruction et le président de la chambre de l'instruction peuvent faire procéder à toutes les vérifications qu'ils estiment nécessaires.

Titre XIX : De la procédure applicable aux infractions de nature sexuelle et de la protection des mineurs victimes

Chapitre II : Du fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes

- **Article 706-53-10**

Modifié par loi n°2010-242 du 10 mars 2010 - art. 12

Toute personne dont l'identité est inscrite dans le fichier peut demander au procureur de la République de rectifier ou d'ordonner l'effacement des informations la concernant si les informations ne sont pas exactes ou si leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier, au regard de la nature de l'infraction, de l'âge de la personne lors de sa commission, du temps écoulé depuis lors et de la personnalité actuelle de l'intéressé.

La demande d'effacement est irrecevable tant que les mentions concernées sont relatives à une procédure judiciaire qui est toujours en cours, tant que la personne n'a pas été réhabilitée ou que la mesure à l'origine de l'inscription n'a pas été effacée du bulletin n° 1.

Si le procureur de la République n'ordonne pas la rectification ou l'effacement, la personne peut saisir à cette fin le juge des libertés et de la détention, dont la décision peut être contestée devant le président de la chambre de l'instruction.

Avant de statuer sur la demande de rectification ou d'effacement, le procureur de la République, le juge des libertés et de la détention et le président de la chambre de l'instruction peuvent faire procéder à toutes les vérifications qu'ils estiment nécessaires et notamment ordonner une expertise médicale de la personne. S'il s'agit d'une mention concernant soit un crime, soit un délit puni de dix ans d'emprisonnement et commis contre un mineur, la décision d'effacement du fichier ne peut intervenir en l'absence d'une telle expertise.

Dans le cas prévu au cinquième alinéa de l'article 706-53-5, le procureur de la République, le juge des libertés et de la détention et le président de la chambre de l'instruction, saisis en application des dispositions du présent article, peuvent également ordonner, à la demande de la personne, qu'elle ne sera tenue de se présenter auprès des services de police ou de gendarmerie pour justifier de son adresse qu'une fois par an ou, lorsqu'elle devait se présenter une fois par mois, qu'une fois tous les six mois.

Titre XX : Du fichier national automatisé des empreintes génétiques

- **Article 706-54**

Créé par loi n°2003-239 du 18 mars 2003 - art. 29

Modifié par loi n°2011-267 du 14 mars 2011 - art. 9

Le fichier national automatisé des empreintes génétiques, placé sous le contrôle d'un magistrat, est destiné à centraliser les empreintes génétiques issues des traces biologiques ainsi que les empreintes génétiques des personnes déclarées coupables de l'une des infractions mentionnées à l'article 706-55 en vue de faciliter l'identification et la recherche des auteurs de ces infractions. Sont conservées dans les mêmes conditions les empreintes génétiques des personnes poursuivies pour l'une des infractions mentionnées à l'article 706-55 ayant fait l'objet d'une décision d'irresponsabilité pénale en application des articles 706-120, 706-125, 706-129, 706-133 ou 706-134.

Les empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 sont également conservées dans ce fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction ; il est fait mention de cette décision au dossier de la procédure. Ces empreintes sont effacées sur instruction du procureur de la République agissant soit d'office, soit à la demande de l'intéressé, lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier. Lorsqu'il est saisi par l'intéressé, le procureur de la République informe celui-ci de la suite qui a été réservée à sa demande ; s'il n'a pas ordonné l'effacement, cette personne peut saisir à cette fin le juge des libertés et de la détention, dont la décision peut être contestée devant le président de la chambre de l'instruction.

Les officiers de police judiciaire peuvent également, d'office ou à la demande du procureur de la République ou du juge d'instruction, faire procéder à un rapprochement de l'empreinte de toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis l'une des infractions mentionnées à l'article 706-55 avec les données incluses au fichier, sans toutefois que cette empreinte puisse y être conservée.

Le fichier prévu par le présent article contient également les empreintes génétiques recueillies à l'occasion :

1° Des procédures de recherche des causes de la mort ou de recherche des causes d'une disparition prévues par les articles 74, 74-1 et 80-4 ;

2° Des recherches aux fins d'identification, prévues par l'article 16-11 du code civil, de personnes décédées dont l'identité n'a pu être établie, à l'exception des militaires décédés à l'occasion d'une opération conduite par les forces armées ou les formations rattachées. Toutefois, les empreintes génétiques recueillies dans ce cadre font l'objet d'un enregistrement distinct de celui des autres empreintes génétiques conservées dans le fichier. Elles sont effacées sur instruction du procureur de la République, agissant soit d'office, soit à la demande des intéressés, lorsqu'il est mis fin aux recherches d'identification qui ont justifié leur recueil. Les empreintes génétiques des ascendants, descendants et collatéraux des personnes dont l'identification est recherchée ne peuvent être conservées dans le fichier que sous réserve du consentement éclairé, exprès et écrit des intéressés.

Les empreintes génétiques conservées dans ce fichier ne peuvent être réalisées qu'à partir de segments d'acide désoxyribonucléique non codants, à l'exception du segment correspondant au marqueur du sexe.

Un décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés détermine les modalités d'application du présent article. Ce décret précise notamment la durée de conservation des informations enregistrées.

Partie réglementaire - Décrets en Conseil d'Etat

Livre Ier : De l'exercice de l'action publique et de l'instruction

Titre IV : Dispositions communes

Chapitre II : Des fichiers de police judiciaire

Section 1 : Du traitement d'antécédents judiciaires

- **Article R. 40-23**

Créé par décret n°2012-652 du 4 mai 2012 - art. 1

Le ministre de l'intérieur (direction générale de la police nationale et direction générale de la gendarmerie nationale) est autorisé à mettre en œuvre un traitement automatisé de données à caractère personnel, dénommé " traitement d'antécédents judiciaires ", dont les finalités sont celles mentionnées à l'article 230-6.

- **Article R. 40-24**

Modifié par décret n°2017-1217 du 2 août 2017 - art. 1

Le traitement est constitué des données recueillies dans le cadre des procédures établies par les services de la police et les unités de la gendarmerie nationales, ou par des agents des douanes habilités à exercer des missions de police judiciaire.

Il peut contenir des données à caractère personnel de la nature de celles mentionnées au I de l'article 8 de la loi du 6 janvier 1978, dans les seuls cas où ces données résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes, dès lors que ces éléments sont nécessaires à la mise en œuvre des finalités mentionnées à l'article 230-6.

En tant que de besoin, et dans le cadre des engagements internationaux en vigueur, le traitement est également constitué des données à caractère personnel issues des traitements gérés par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers.

- **Article R. 40-25**

Créé par décret n°2012-652 du 4 mai 2012 - art. 1

Les données recueillies dans le cadre de l'article R. 40-24 ne peuvent concerner que les catégories suivantes :

1° Les personnes à l'encontre desquelles sont réunis, lors de l'enquête préliminaire, de l'enquête de flagrance ou sur commission rogatoire, des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission d'un crime, d'un délit ou d'une contravention de cinquième classe prévue aux articles R. 625-1 à R. 625-3, R. 625-7, R. 625-9, R. 635-1, R. 635-3 à R. 635-5, R. 645-1, R. 645-2 et R. 645-5 à R. 645-15 du code pénal ;

2° Les victimes de ces infractions ;

3° Les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition au sens des articles 74 et 74-1.

- **Article R. 40-26**

Modifié par décret n°2017-1217 du 2 août 2017 - art. 2

Peuvent être enregistrées dans le présent traitement les catégories de données à caractère personnel et informations suivantes :

1° Concernant les personnes mises en cause :

a) Personnes physiques :

– identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe) ;

– surnom, alias ;

– date et lieu de naissance ;

– situation familiale ;

– filiation ;

– nationalité ;

– adresses ;

– adresses de messagerie électronique ;

– numéros de téléphone ;

– profession ;

– état de la personne ;

– signalement ;

– photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale (photographie du visage de face) ;

– autres photographies ;

b) Personnes morales :

– raison sociale, enseigne commerciale, sigle ;

- forme juridique ;
- numéro d'inscription au registre du commerce et des sociétés ;
- lieu du siège social ;
- numéro SIREN, SIRET ;
- secteur d'activité ;
- adresses ;
- adresses de messagerie électronique ;
- numéros de téléphone.

2° Concernant les victimes :

a) Personnes physiques :

- identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe) ;
- date et lieu de naissance ;
- situation familiale ;
- nationalité ;
- adresses ;
- adresses de messagerie électronique ;
- numéros de téléphone ;
- profession ;
- état de la personne ;

b) Personnes morales :

- raison sociale, enseigne commerciale, sigle ;
- forme juridique ;
- numéro d'inscription au registre du commerce et des sociétés ;
- secteur d'activité ;
- lieu du siège social ;
- adresses ;
- adresses de messagerie électronique ;
- numéros de téléphone.

3° Concernant les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition :

- identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe) ;
- date et lieu de naissance ;
- situation familiale ;
- nationalité ;
- adresses ;
- adresses de messagerie électronique ;
- numéros de téléphone ;
- profession ;
- état de la personne ;
- signalement (personnes disparues et corps non identifiés) ;
- photographie comportant les caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale (photographie du visage de face des personnes disparues et corps non identifiés) ;
- photographies (personnes disparues et corps non identifiés).

Sont également enregistrées les données à caractère non personnel qui concernent les faits, objets de l'enquête, les lieux, dates de l'infraction et modes opératoires ainsi que les données et images relatives aux objets, y compris celles qui permettent indirectement d'identifier les personnes concernées.

- **Article R. 40-27**

Modifié par décret n°2017-1217 du 2 août 2017 - art. 3

I. – Les données concernant la personne mise en cause majeure sont conservées vingt ans.

Par dérogation, elles sont conservées :

– cinq ans lorsque la personne est mise en cause pour l'un des délits prévus par le code de la route ou aux articles 221-6,221-6-1,222-19,222-19-1,222-20-1,225-10-1 ,227-3 à 227-11,311-3,314-5 ,314-6,431-1,431-4 et 434-10 du code pénal et L. 3421-1 du code de la santé publique, ainsi que pour les contraventions énumérées à l'article R. 40-25 ;

– quarante ans lorsque la personne est mise en cause pour l'une des infractions figurant au tableau 1 ci-dessous.

II. – Les données concernant la personne mise en cause mineure sont conservées cinq ans.

Par dérogation, elles sont conservées :

– dix ans lorsque la personne est mise en cause pour l'une des infractions figurant au tableau 2 ci-dessous ;

– vingt ans lorsque la personne est mise en cause pour l'une des infractions figurant au tableau 3 ci-dessous.

III. – En cas de mise en cause pour une ou plusieurs nouvelles infractions avant l'expiration de l'une des durées, fixées au I et au II, de conservation des données initiales, le délai de conservation restant le plus long s'applique aux données concernant l'ensemble des infractions pour lesquelles la personne a été mise en cause.

IV. – La durée de conservation des données à caractère personnel concernant les victimes est au maximum de quinze ans.

V. – Les données à caractère personnel concernant les personnes mentionnées au 3° de l'article R. 40-25 sont effacées lorsque l'enquête a permis de retrouver la personne disparue ou d'écartier toute suspicion de crime ou délit.

Tableau 1. – Liste des infractions permettant de conserver quarante ans les données concernant les personnes mises en cause majeures

Infraction contre les personnes :

- administration de substances nuisibles ;
- détournement de moyen de transport ;
- empoisonnement ;
- enlèvement, séquestration, prise d'otage ;
- exploitation de la mendicité aggravée ou en bande organisée ;
- crime contre l'humanité, génocide ;
- meurtre, assassinat ;
- menace de mort, menace de destruction, dégradation ou détérioration dangereuse pour les personnes ;
- torture, acte de barbarie ;
- violence volontaire ayant entraîné la mort ;
- violence volontaire entraînant une mutilation ou une infirmité permanente ;
- vol avec violences ;
- agression sexuelle ;
- atteinte sexuelle sur mineur de quinze ans, atteinte sexuelle sur mineur de plus de quinze ans aggravée ;
- corruption de mineur ;
- proxénétisme ;
- viol ;
- trafic de stupéfiants ;
- traite des êtres humains.

Infractions contre les biens :

- abus de confiance aggravé ;
- destruction, dégradation et détérioration d'un bien appartenant à autrui par l'effet d'une substance explosive, d'un incendie ou de tout autre moyen de nature à créer un danger pour les personnes ;
- escroquerie aggravée ;

- extorsion ;
- vol en bande organisée ;
- vol avec arme ;
- blanchiment ;
- contrefaçon, falsification de monnaies et moyens de paiement ;
- faux en écritures publiques ;
- abus de biens sociaux ;
- délit d'initié ;
- atteinte aux systèmes de traitement automatisé des données.

Atteintes à la paix publique :

- acte de terrorisme ;
- association de malfaiteurs ;
- évasion ;
- infraction au régime des armes et munitions à l'exception du port ou transport d'arme de catégorie D ;
- atteinte aux intérêts fondamentaux de la Nation ;
- recel de malfaiteurs ;
- violation de secret (professionnel, de fabrique).

Tableau 2. – Liste des infractions permettant de conserver dix ans les données concernant les personnes mises en cause mineures

Infractions contre les personnes :

- exploitation de la mendicité aggravée ou en bande organisée ;
- vol avec violences ;
- violence volontaire aggravée autres que celles prévues au tableau 3 ;
- transport, détention, offre, cession, acquisition ou emploi illicites de stupéfiants ;
- traite des êtres humains autre que celle prévue au tableau 3 ;
- exhibition sexuelle.

Infractions contre les biens :

- destruction, dégradation et détérioration d'un bien appartenant à autrui par l'effet d'une substance explosive, d'un incendie ou de tout autre moyen de nature à créer un danger pour les personnes ;
- extorsion ;
- atteinte aux systèmes de traitement automatisé de données ;
- blanchiment ;
- contrefaçon, falsification de monnaies ou moyens de paiement.

Atteintes à la paix publique :

Recel de malfaiteurs.

Tableau 3. – Liste des infractions permettant de conserver vingt ans les données concernant les personnes mises en cause mineures

Infractions contre les personnes :

- administration de substances nuisibles ;
- détournement de moyen de transport ;
- empoisonnement ;
- enlèvement, séquestration, prise d'otage ;
- crime contre l'humanité, génocide ;
- meurtre, assassinat ;
- torture, acte de barbarie ;
- violence volontaire ayant entraîné la mort ;

- violence volontaire entraînant une mutilation ou une infirmité permanente ;
 - vol avec violences aggravé ;
 - agression sexuelle ;
 - proxénétisme ;
 - viol ;
 - trafic de stupéfiants autres que ceux visés au tableau 2 ;
 - traite des êtres humains en bande organisée ou avec tortures et actes de barbarie.
- Infractions contre les biens :
- vol en bande organisée ;
 - vol avec arme.
- Atteintes à la paix publique :
- acte de terrorisme ;
 - association de malfaiteurs ;
 - atteinte aux intérêts fondamentaux de la Nation.

- **Article R. 40-28**

Modifié par décret n°2017-1217 du 2 août 2017 - art. 4

I. – Ont accès à la totalité ou, à raison de leurs attributions, à une partie des données mentionnées à l'article R. 40-26 pour les besoins des enquêtes judiciaires :

1° Les agents des services de la police nationale exerçant des missions de police judiciaire individuellement désignés et spécialement habilités soit par les chefs des services territoriaux de la police nationale, soit par les chefs des services actifs à la préfecture de police ou, le cas échéant, le préfet de police, soit par les chefs des services centraux de la police nationale ou, le cas échéant, le directeur général dont ils relèvent ;

2° Les militaires des unités de la gendarmerie nationale exerçant des missions de police judiciaire individuellement désignés et spécialement habilités soit par les commandants de groupement, soit par les commandants de la gendarmerie dans les départements et les collectivités outre-mer et en Nouvelle-Calédonie, soit par les commandants de région, soit par les commandants des gendarmeries spécialisées, soit par le sous-directeur de la police judiciaire ou, le cas échéant, par le directeur général de la gendarmerie nationale ;

3° Les agents du service national de la douane judiciaire, dans le cadre de leurs attributions légales, individuellement désignés et spécialement habilités par le magistrat délégué aux missions judiciaires de la douane ou, le cas échéant, par le directeur général des douanes et droits indirects ;

4° Les magistrats du parquet ;

5° Les agents des services judiciaires, individuellement désignés et spécialement habilités par le procureur de la République, chargés d'indiquer au gestionnaire du traitement les décisions judiciaires et requalifications donnant lieu, dans les conditions définies à l'article R. 40-31, à mise à jour ou effacement des données.

6° Le magistrat mentionné à l'article 230-9 ainsi que les agents des services judiciaires individuellement désignés et spécialement habilités par ce magistrat, chargés de l'instruction des demandes de rectification et d'effacement ;

7° Les agents affectés dans les services de la police nationale chargés d'une mission de police judiciaire, individuellement désignés et spécialement habilités soit par les chefs des services territoriaux, soit par les chefs de services actifs à la préfecture de police, ou le cas échéant, le préfet de police, soit par les chefs des services centraux de la police nationale, ou le cas échéant, le directeur général dont ils relèvent, pour les besoins de la collecte, de la vérification, de la mise à jour ou de l'effacement des données enregistrées dans le traitement ;

8° Les agents des unités de la gendarmerie nationale exerçant des missions de police judiciaire individuellement désignés et spécialement habilités soit par les commandants de groupement, soit par les commandants de la gendarmerie dans les départements et les collectivités outre-mer et en Nouvelle-Calédonie, soit par les commandants de région, soit par les commandants des gendarmeries spécialisées, soit par le sous-directeur de la police judiciaire ou, le cas échéant, par le directeur général de la gendarmerie nationale, pour les besoins de la collecte, de la vérification, de la mise à jour ou de l'effacement des données enregistrées dans le traitement ;

L'accès par tous moyens techniques mobiles aux données du fichier est ouvert aux seules personnes mentionnées aux 1°, 2° et 3°.

II. – Peuvent être destinataires des mêmes données :

1° Les autres agents de l'Etat investis par la loi d'attributions de police judiciaire ;

2° Les magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis ;

3° Les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers, dans les conditions énoncées à l'article L. 235-1 du code de la sécurité intérieure.

Seules les informations enregistrées dans le traitement relatives à la procédure en cours peuvent être jointes au dossier de la procédure.

- **Article R. 40-29**

Modifié par décret n°2017-1217 du 2 août 2017 - art. 5

I. – Dans le cadre des enquêtes prévues à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995, aux articles L. 114-1, L. 114-2, L. 211-11-1, L. 234-1 et L. 234-2 du code de la sécurité intérieure et à l'article L. 4123-9-1 du code de la défense, les données à caractère personnel figurant dans le traitement qui se rapportent à des procédures judiciaires en cours ou closes, à l'exception des cas où sont intervenues des mesures ou décisions de classement sans suite, de non-lieu, de relaxe ou d'acquiescement devenues définitives, ainsi que des données relatives aux victimes, peuvent être consultées, sans autorisation du ministère public, par :

1° Les personnels de la police et de la gendarmerie habilités selon les modalités prévues au 1° et au 2° du I de l'article R. 40-28 ;

2° Les agents individuellement désignés et spécialement habilités des services spécialisés de renseignement mentionnés à l'article R. 234-2 du code de la sécurité intérieure ;

3° Les agents du service à compétence nationale dénommé “ service national des enquêtes administratives de sécurité ”, individuellement désignés et spécialement habilités par le directeur général de la police nationale ;

4° Les agents du service à compétence nationale dénommé “ Commandement spécialisé pour la sécurité nucléaire ”, individuellement désignés et spécialement habilités par le directeur général de la gendarmerie nationale ;

5° Les personnels investis de missions de police administrative individuellement désignés et spécialement habilités par le représentant de l'Etat. L'habilitation précise limitativement les motifs qui peuvent justifier pour chaque personne les consultations autorisées. Lorsque la consultation révèle que l'identité de la personne concernée a été enregistrée dans le traitement en tant que mise en cause, l'enquête administrative ne peut aboutir à un avis ou une décision défavorables sans la saisine préalable, pour complément d'information, des services de la police nationale ou des unités de la gendarmerie nationale compétents et, aux fins de demandes d'information sur les suites judiciaires, du ou des procureurs de la République compétents. Le procureur de la République adresse aux autorités gestionnaires du traitement un relevé des suites judiciaires devant figurer dans le traitement d'antécédents judiciaires et relatif à la personne concernée. Il indique à l'autorité de police administrative à l'origine de la demande si ces données sont accessibles en application de l'article 230-8 du présent code.

II. – Dans le cadre des missions ou interventions prévues à l'article L. 234-3 du code de la sécurité intérieure, les données à caractère personnel figurant dans le traitement qui se rapportent à des procédures judiciaires en cours ou closes, à l'exception des cas où sont intervenues des mesures ou décisions de classement sans suite, de non-lieu, de relaxe ou d'acquiescement devenues définitives, ainsi que des données relatives aux victimes, peuvent être consultées, sans autorisation du ministère public, par les personnels de la police et de la gendarmerie habilités selon les modalités prévues au 1° et au 2° du I de l'article R. 40-28.

Cette consultation peut également être effectuée, dans les mêmes conditions qu'à l'alinéa précédent, par les agents des services de renseignement désignés par le ministre de la défense, aux seules fins de protection de la sécurité de leurs personnels. Ces agents sont individuellement désignés et spécialement habilités par leurs directeurs respectifs.

III. – Peuvent être destinataires des données mentionnées au I, pour l'exercice de leurs missions en matière de police administrative et dans la limite du besoin d'en connaître, les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers dans les conditions énoncées à l'article L. 235-1 du code de la sécurité intérieure.

- **Article R. 40-29-1**

Créé par décret n°2017-1217 du 2 août 2017 - art. 6

Peuvent avoir accès, aux seules fins de consultation, aux données à caractère personnel figurant dans le traitement, à l'exclusion de celles relatives aux personnes enregistrées en qualité de victimes :

1° Les agents des services mentionnés à l'article R. 234-3 du code de la sécurité intérieure, individuellement désignés et habilités par le directeur dont ils relèvent, dans les conditions prévues à l'article L. 234-4 du même code ;

2° Les agents du service mentionné à l'article L. 561-23 du code monétaire et financier, individuellement désignés et habilités par le directeur du service, dans les conditions prévues à l'article L. 561-27 du même code.

Article R40-30 En savoir plus sur cet article...

Créé par Décret n°2012-652 du 4 mai 2012 - art. 1

Les consultations effectuées font l'objet d'un enregistrement comprenant l'identifiant du consultant, la date et l'heure de la consultation ainsi que sa nature administrative ou judiciaire. Ces données sont conservées cinq ans.

- **Article R. 40-31**

Modifié par Décret n°2017-1217 du 2 août 2017 - art. 7

Le traitement des données à caractère personnel fait l'objet du contrôle et du suivi prévus aux articles 230-8 et 230-9.

Les demandes de rectification ou d'effacement des données émanant des personnes intéressées peuvent être adressées soit directement au procureur de la République territorialement compétent ou au magistrat mentionné à l'article 230-9 soit, par l'intermédiaire de la Commission nationale de l'informatique et des libertés, au responsable du traitement. Toute demande de rectification ou d'effacement adressée au procureur de la République territorialement compétent ou au magistrat mentionné à l'article 230-9 doit, à peine d'irrecevabilité, être adressée par lettre recommandée avec demande d'avis de réception.

Les personnes morales ne peuvent présenter leur demande que directement auprès du procureur de la République.

Si le procureur de la République ou le responsable du traitement saisi constate que les données dont il est demandé la mise à jour sont issues de procédures diligentées sur plusieurs ressorts, il adresse la demande au magistrat mentionné à l'article 230-9.

- **Article R. 40-31-1**

Créé par Décret n°2017-1217 du 2 août 2017 - art. 8

Lorsqu'il est saisi d'une demande de rectification ou d'effacement, le procureur de la République territorialement compétent ou le magistrat mentionné à l'article 230-9 fait connaître sa décision à l'intéressé, par lettre recommandée.

Si le procureur de la République territorialement compétent ou le magistrat mentionné à l'article 230-9 n'ordonne pas l'effacement ou la rectification, l'intéressé peut, en application du troisième alinéa de l'article 230-8 et du quatrième alinéa de l'article 230-9, saisir respectivement le président de la chambre de l'instruction ou le président de la chambre de l'instruction de la cour d'appel de Paris, dans un délai d'un mois à compter de l'envoi de la décision de refus, par lettre recommandée avec demande d'avis de réception ou par déclaration au greffe de la chambre de l'instruction. A peine d'irrecevabilité, sa contestation doit être motivée.

Si le procureur de la République territorialement compétent ou le magistrat mentionné à l'article 230-9 ne se prononce pas dans un délai de deux mois, l'intéressé peut, dans un délai d'un mois, saisir respectivement le président de la chambre de l'instruction ou le président de la chambre de l'instruction de la cour d'appel de Paris de cette décision implicite de rejet en application de l'article 802-1 du présent code. Le procureur de la République territorialement compétent ou le magistrat mentionné à l'article 230-9 est informé sans délai et par tous moyens de l'exercice de ce recours. Ce recours devient caduc si le procureur de la République territorialement compétent ou le magistrat mentionné à l'article 230-9 fait droit à la demande de l'intéressé.

Le président de la chambre de l'instruction statue, après avoir sollicité les réquisitions écrites du procureur général, par une ordonnance motivée, dans un délai de six mois à compter de la date de réception de la lettre recommandée ou de la déclaration au greffe par le requérant. Cette ordonnance est portée à la connaissance du

procureur de la République territorialement compétent ou du magistrat mentionné à l'article 230-9 et notifiée par lettre recommandée à l'intéressé. Elle ne peut faire l'objet d'un pourvoi en cassation que si elle ne satisfait pas, en la forme, aux conditions essentielles de son existence légale.

- **Article R. 40-32**

Créé par décret n°2012-652 du 4 mai 2012 - art. 1

La mise en œuvre et la mise à jour du traitement sont contrôlées par un magistrat du parquet hors hiérarchie, désigné pour trois ans par arrêté du garde des sceaux, ministre de la justice, et assisté par un comité composé de trois membres nommés dans les mêmes conditions.

Les autorités gestionnaires du traitement lui adressent, sur sa demande, toutes informations relatives à ce traitement.

Ce magistrat peut ordonner toutes mesures nécessaires à l'exercice de son contrôle.

Il établit un rapport annuel qu'il adresse au ministre de la justice ; il en adresse aussi copie aux autorités gestionnaires du traitement.

Les pouvoirs qui lui sont confiés s'exercent sans préjudice du contrôle exercé par la Commission nationale de l'informatique et des libertés en application des dispositions et selon les modalités prévues par les articles 41 et 44 de la loi n° 78-17 du 6 janvier 1978.

- **Article R. 40-33**

Créé par décret n°2012-652 du 4 mai 2012 - art. 1

I. — Le droit d'accès s'exerce de manière indirecte, dans les conditions prévues à l'article 41 de la loi n° 78-17 du 6 janvier 1978, par demande portée préalablement devant la Commission nationale de l'informatique et des libertés, pour l'ensemble des données.

La Commission peut constater, en accord avec le responsable du traitement, que des données à caractère personnel enregistrées ne mettent pas en cause la sûreté de l'Etat, la défense ou la sécurité publique et qu'il y a donc lieu de les communiquer à la personne intéressée, après accord du procureur de la République lorsque la procédure n'est pas judiciairement close.

II. — Le droit d'opposition prévu à l'article 38 de la même loi ne s'applique pas au présent traitement.

Toute personne identifiée dans le fichier en qualité de victime peut cependant s'opposer à ce que des données à caractère personnel la concernant soient conservées dans le fichier dès lors que l'auteur des faits a été condamné définitivement.

III. — Les personnes mentionnées au 2° de l'article R. 40-25 sont informées des droits d'accès et d'opposition qui leur sont ouverts en application du I et du II du présent article.

- **Article R. 40-34**

Créé par décret n°2012-652 du 4 mai 2012 - art. 1

Sans préjudice de l'application de l'article 44 de la loi n° 78-17 du 6 janvier 1978, le directeur général de la police nationale et le directeur général de la gendarmerie nationale rendent compte conjointement chaque année à la Commission nationale de l'informatique et des libertés des opérations de vérification, de mise à jour et d'effacement des informations enregistrées dans le traitement.

3. Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité

- **Article 17-1**

Modifié par ordonnance n°2012-351 du 12 mars 2012 - art. 13

Modifié par ordonnance n°2012-351 du 12 mars 2012 - art. 19 (V)

Il est procédé à la consultation prévue à l'article L. 234-1 du code de la sécurité intérieure pour l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux.

D. Application des dispositions contestées

1. Jurisprudence

a. Jurisprudence de la CEDH

- **CEDH, 26 mars 1987, *Leander c. Suède*, n° 9248/81**

A. Sur l'existence d'une ingérence dans l'exercice d'un droit garanti par l'article 8 (art. 8)

48. Le registre secret de la police renfermait sans contredit des données relatives à la vie privée de M. Leander. Tant leur mémorisation que leur communication, assorties du refus d'accorder à M. Leander la faculté de les réfuter, portaient atteinte à son droit au respect de sa vie privée, garanti par l'article 8 par. 1 (art. 8-1).

- **CEDH, 16 février 2000, *Amann c. Suisse*, n° 27798/ 95**

II. Sur la violation alléguée de l'article 8 de la Convention quant à l'établissement d'une fiche et sa conservation dans le fichier de la confédération

64. Le requérant se plaint de ce que l'établissement d'une fiche le concernant, à la suite de l'interception de l'appel téléphonique reçu d'une personne de l'ambassade alors soviétique à Berne, et sa conservation dans le fichier de la Confédération ont entraîné une violation de l'article 8 de la Convention.

A. Applicabilité de l'article 8

65. La Cour rappelle que la mémorisation de données relatives à la « vie privée » d'un individu entre dans le champ d'application de l'article 8 § 1 (arrêt *Leander c. Suède* du 26 mars 1987, série A n° 116, p. 22, § 48).

A cet égard, elle souligne que le terme « vie privée » ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables ; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de « vie privée » (arrêts *Niemietz c. Allemagne* du 16 décembre 1992, série A n° 251-B, pp. 33-34, § 29, et *Halford* précité, pp. 1015-1016, § 42).

Cette interprétation extensive concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, entrée en vigueur le 1er octobre 1985, dont le but est « de garantir, sur le territoire de chaque Partie, à toute personne physique (...) le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1), ces dernières étant définies comme « toute information concernant une personne physique identifiée ou identifiable » (article 2).

66. En l'espèce, la Cour relève qu'une fiche a été établie concernant le requérant, sur laquelle il a été indiqué que ce dernier était un « contact auprès de l'ambassade russe » et faisait « du commerce de différentes sortes avec la société [A.] » (paragraphes 15 et 18 ci-dessus).

67. Pour la Cour, il s'agit là sans contredit de données relatives à la « vie privée » du requérant et l'article 8 trouve en conséquence à s'appliquer à ce grief également.

B. Observation de l'article 8

1. Sur l'existence d'une ingérence

68. Pour le Gouvernement, la question de savoir s'il y a eu « ingérence » au sens de l'article 8 de la Convention demeure posée, puisque « la fiche ne contenait aucun élément sensible en rapport avec la vie privée du requérant », que ce dernier « n'a subi aucun inconvénient du fait de l'établissement et de la conservation de la fiche » et que celle-ci n'a « très probablement jamais été consultée par des tiers ».

69. La Cour rappelle que la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu (voir, mutatis mutandis, arrêts Leander précité, p. 22, § 48, et Kopp précité, p. 540, § 53).

70. En l'espèce, la Cour relève qu'une fiche contenant des données relatives à la vie privée du requérant a été établie par le ministère public, puis conservée dans le fichier de la Confédération. A cet égard, elle souligne qu'il ne lui appartient pas de spéculer sur le caractère sensible ou non des éléments recueillis ni sur les éventuels inconvénients subis par le requérant. Il lui suffit de constater que des données relatives à la vie privée d'un particulier ont été mémorisées par une autorité publique pour conclure qu'en l'espèce, l'établissement et la conservation de la fiche litigieuse constituent une ingérence, au sens de l'article 8, dans le droit au respect de la vie privée du requérant.

2. Justification de l'ingérence

71. Pareille ingérence méconnaît l'article 8 sauf si, « prévue par la loi », elle poursuit un ou des buts légitimes au regard du paragraphe 2 et, de surcroît, est « nécessaire dans une société démocratique » pour atteindre ces derniers.

a) L'ingérence était-elle « prévue par la loi » ?

72. Selon le requérant, l'établissement et la conservation de la fiche le concernant sont des mesures qui ne reposent pas sur une base légale. En particulier, il affirme que l'article 17 § 3 PPF n'autorise pas la police fédérale à consigner les résultats de ses mesures de surveillance. Quant aux directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale, elles sont destinées aux fonctionnaires de l'administration et il ne s'agit donc pas d'une loi suffisamment claire et précise pour permettre aux citoyens de déterminer leurs droits et obligations.

Il soutient que de surcroît les autorités ne se sont pas conformées aux normes en vigueur, puisque l'article 66 § 1 ter PPF et le chiffre 414 des directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale exigeaient la destruction des enregistrements ne s'avérant pas nécessaires pour l'exécution d'une enquête.

Enfin, il souligne que la législation entrée en vigueur au début des années 90, après l'éclatement de l'affaire dite « des fiches », ne prévoit pas la possibilité d'engager une procédure judiciaire aux fins d'obtenir la destruction d'une fiche. Ainsi, aux termes de l'arrêté fédéral du 9 octobre 1992 sur la consultation des documents du ministère public de la Confédération et de l'ordonnance du Conseil fédéral du 20 janvier 1993 sur la consultation des documents du ministère public de la Confédération, les fiches sont conservées dans les archives fédérales et il est seulement loisible aux justiciables d'y faire annoter une remarque lorsque le contenu en est contesté.

73. La Commission partage l'opinion du requérant. En particulier, elle estime que les directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale ne sont pas assez précises et se contentent de présupposer, sans en donner une elles-mêmes, une base légale à la mémorisation d'informations.

74. Le Gouvernement soutient que l'ordre juridique suisse offre, compte tenu « des particularités caractérisant les mesures secrètes dans le domaine de la protection de la sécurité de l'Etat », une base légale suffisamment accessible et prévisible.

Il est d'avis qu'avant 1990, les mesures litigieuses étaient principalement fondées sur les articles 17 § 3 PPF et premier de l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral, ces dispositions étant concrétisées par les directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale. Il précise que ces directives ont été publiées dans la Feuille fédérale (FF 1981, I, p. 1314).

Il indique qu'après 1990, plusieurs textes ont été édictés en matière de traitement et de consultation de documents contenant des données personnelles, en particulier l'ordonnance du Conseil fédéral du 5 mars 1990 relative au traitement des documents de la Confédération établis pour assurer la protection de l'Etat, l'arrêté fédéral du 9 octobre 1992 sur la consultation des documents du ministère public de la Confédération et l'ordonnance du Conseil fédéral du 20 janvier 1993 sur la consultation des documents du ministère public de la Confédération.

i. L'établissement de la fiche

75. La Cour relève qu'en décembre 1981, date à laquelle fut établie la fiche concernant le requérant, la loi fédérale sur la procédure pénale, l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral et les directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale étaient en vigueur. Toutefois, aucun de ces textes ne mentionnant expressément l'existence d'un registre du ministère public, la question pourrait se poser de savoir

si la rédaction de la fiche litigieuse reposait sur « une base légale en droit suisse » et, dans l'affirmative, si cette dernière était « accessible » (arrêt Leander précité, p. 23, § 51). A cet égard, elle observe en effet que les directives du Conseil fédéral du 16 mars 1981 étaient avant tout destinées au personnel de l'administration fédérale.

En l'espèce, cependant, elle n'estime pas nécessaire de se prononcer à ce sujet, puisqu'à supposer même que l'établissement de la fiche, en décembre 1981, fût fondé sur une base légale accessible, celle-ci n'était pas « prévisible ».

76. La Cour a jugé ci-dessus (paragraphe 58 et 59) que les articles 17 § 3 PPF et premier de l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral étaient rédigés en termes trop généraux pour satisfaire à l'exigence de prévisibilité en matière d'écoutes téléphoniques. Pour les motifs déjà exposés, elle aboutit à la même conclusion concernant la création de la fiche sur le requérant.

Quant aux directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale, elles énoncent quelques principes généraux, par exemple que le « traitement de données personnelles doit reposer sur une base légale » (chiffre 411) ou que les « données personnelles ne doivent être traitées que dans des buts bien déterminés » (chiffre 412), mais ne contiennent aucune indication appropriée sur l'étendue et les modalités d'exercice du pouvoir conféré au ministère public de recueillir, enregistrer et conserver des informations ; ainsi, elles ne précisent pas les conditions d'établissement des fiches, les procédures à suivre, les informations pouvant être mémorisées et les mentions éventuellement interdites.

Ces directives, à l'instar de la loi fédérale sur la procédure pénale et l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral, ne sauraient en conséquence être considérées comme suffisamment claires et détaillées pour assurer une protection adéquate contre les ingérences des autorités dans le droit du requérant au respect de sa vie privée.

77. L'établissement de la fiche concernant le requérant n'était donc pas « prévu par la loi » au sens de l'article 8 de la Convention.

ii. La conservation de la fiche

78. La Cour souligne d'abord qu'il paraît douteux que la conservation d'une fiche dont la création n'a pas été « prévue par la loi » puisse satisfaire à cette exigence.

De surcroît, elle relève que le droit suisse, et ce tant avant qu'après 1990, prévoit expressément la destruction des données qui ne s'avèrent plus « nécessaires » ou sont devenues « inutiles » (article 66 § 1 ter PPF, chiffre 414 des directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale et article 7 de l'arrêté fédéral du 9 octobre 1992 sur la consultation des documents du ministère public de la Confédération).

Or, en l'espèce, les autorités n'ont pas détruit les renseignements mémorisés lorsqu'il s'est avéré qu'aucune infraction n'était en cours de préparation, comme le souligne le Tribunal fédéral dans son arrêt du 14 septembre 1994.

79. Pour ces motifs, la conservation de la fiche concernant le requérant n'était pas « prévue par la loi » au sens de l'article 8 de la Convention.

80. La Cour conclut que tant l'établissement de la fiche litigieuse par le ministère public que la conservation de cette dernière dans le fichier de la Confédération constituent des ingérences dans la vie privée du requérant qui ne sauraient passer pour « prévues par la loi » puisque le droit suisse n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. Il s'ensuit qu'il y a eu violation de l'article 8 de la Convention.

b) Finalité et nécessité de l'ingérence

81. Eu égard à la conclusion qui précède, la Cour n'estime pas nécessaire d'examiner le respect des autres exigences du paragraphe 2 de l'article 8.

- **CEDH, 4 décembre 2008, S. et Marper c. Royaume-Uni, n° 30562/04 et 30566/04**

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

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

« 1. Toute personne a droit au respect de sa vie privée (...)

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 défense de l'ordre et à la prévention des infractions pénales (...) »

A. Existence d'une ingérence dans la vie privée

59. La Cour recherchera tout d'abord si la conservation par les autorités des empreintes digitales, échantillons cellulaires et profils ADN des requérants peut s'analyser en une ingérence dans la vie privée des intéressés.

1. Les arguments des parties

a. Les requérants

60. Les requérants soutiennent que la conservation de leurs empreintes digitales, échantillons cellulaires et profils ADN est constitutive d'une atteinte à leur droit au respect de leur vie privée. Les éléments en question seraient en effet étroitement liés à leur identité individuelle et représenteraient une catégorie de données à caractère personnel dont ils seraient en droit de garder le contrôle. Ils rappellent que le prélèvement initial de pareilles informations biologiques a toujours été considéré comme faisant entrer en jeu l'article 8 et arguent que leur conservation est encore plus sujette à controverse vu la profusion d'informations privées qui sont ainsi mises en permanence à la disposition d'autrui et échappent au contrôle de la personne concernée. Ils soulignent en particulier la stigmatisation sociale et les conséquences psychologiques que provoquent selon eux la conservation de telles informations lorsqu'il s'agit d'enfants, raison pour laquelle l'atteinte au droit au respect de la vie privée serait encore plus forte en ce qui concerne le premier requérant.

61. Ils voient une corroboration de leur thèse dans la jurisprudence des organes de la Convention, de même que dans une décision récemment adoptée par le Tribunal de l'information au Royaume-Uni (*Chief Constables of West Yorkshire, South Yorkshire and North Wales Police v. the Information Commissioner*, [2005] UK IT EA 2005 0010 (12 octobre 2005), 173). Cette décision se serait appuyée sur l'opinion exprimée par la baronne Hale of Richmond lors de la procédure devant la Chambre des lords (paragraphe 25 ci-dessus) et aurait repris en substance sa conclusion pour trancher une question similaire concernant l'application de l'article 8 à la conservation de données relatives à des condamnations.

62. Les requérants considèrent que la conservation d'échantillons cellulaires s'analyse en une atteinte plus prononcée encore aux droits garantis par l'article 8, pareils échantillons contenant le patrimoine génétique de la personne concernée ainsi que des informations génétiques sur ses proches parents. La question ne serait pas de savoir si des données ont effectivement été extraites des échantillons ou si elles ont causé un préjudice dans un cas particulier, toute personne ayant droit à la garantie que de telles informations faisant partie d'elle-même demeureront privées et ne seront pas communiquées ou rendues accessibles à autrui sans son autorisation.

b. Le Gouvernement

63. Le Gouvernement admet que les empreintes digitales, profils ADN et échantillons sont des « données à caractère personnel » au sens de la loi de 1998 sur la protection des données, qui se trouvent entre les mains de personnes en mesure d'identifier les individus concernés. Il considère toutefois que la seule conservation des empreintes digitales, profils ADN et échantillons aux fins de l'usage limité autorisé par l'article 64 de la loi de 1984 ne relève pas du droit au respect de la vie privée consacré par l'article 8 § 1 de la Convention. A la différence du prélèvement, la conservation de ces données ne porterait pas atteinte à l'intégrité physique et psychologique de la personne et ne méconnaîtrait pas non plus le droit à l'épanouissement personnel, le droit de nouer et développer des relations avec ses semblables ni le droit à l'autodétermination.

64. Le Gouvernement estime qu'en réalité les requérants craignent les utilisations qui pourraient être faites à l'avenir des échantillons stockés, l'apparition de nouvelles méthodes d'analyse des données ADN et le risque d'intervention dans la vie privée des individus par l'intermédiaire d'une surveillance active. Il souligne à cet égard que le champ d'utilisation de ces données est expressément et clairement limité par le cadre législatif, les procédés technologiques d'extraction des profils ADN et la nature des profils ADN obtenus.

65. Un profil ADN ne serait rien de plus qu'une suite de chiffres permettant d'identifier une personne à partir d'échantillons cellulaires et il ne contiendrait aucune information de nature intrusive sur l'individu concerné ou sa personnalité. La base de données ADN serait une collection de profils ADN, lesquels pourraient être ressortis à l'occasion de recherches effectuées à partir d'éléments recueillis sur les lieux d'infractions. Une personne ne serait identifiée que dans le cas d'une concordance de son profil avec l'un de ces éléments et dans la mesure de cette concordance. On ne procéderait à des recherches familiales à partir de concordances partielles que dans des cas extrêmement rares et strictement encadrés. Les empreintes digitales, profils ADN et échantillons ne se prêteraient à aucun commentaire subjectif et ils ne fourniraient pas la moindre information quant aux activités d'une personne ; ils ne risqueraient donc nullement de modifier la perception que l'on peut avoir d'un individu ni de porter atteinte à sa réputation. A supposer même que la conservation de pareils éléments soit susceptible de tomber dans le champ d'application de l'article 8 § 1 de la Convention, le caractère extrêmement limité de

ses conséquences négatives éventuelles obligerait à conclure que cette conservation n'est pas suffisamment grave pour s'analyser comme une ingérence.

2. L'appréciation de la Cour

a. Principes généraux

66. La Cour rappelle que la notion de « vie privée » est une notion large, non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne (*Pretty c. Royaume-Uni*, no 2346/02, § 61, CEDH 2002-III, et *Y.F. c. Turquie*, no 24209/94, § 33, CEDH 2003-IX). Elle peut donc englober de multiples aspects de l'identité physique et sociale d'un individu (*Mikulic c. Croatie*, no 53176/99, § 53, CEDH 2002-I). Des éléments tels, par exemple, l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle relèvent de la sphère personnelle protégée par l'article 8 (voir, entre autres, *Bensaid c. Royaume-Uni*, no 44599/98, § 47, CEDH 2001-I et les références qui y sont citées, et *Peck c. Royaume-Uni*, no 44647/98, § 57, CEDH 2003-I). Au-delà du nom, la vie privée et familiale peut englober d'autres moyens d'identification personnelle et de rattachement à une famille (voir, mutatis mutandis, *Burghartz c. Suisse*, 22 février 1994, § 24, série A no 280-B, et *Ünal Tekeli c. Turquie*, no 29865/96, § 42, CEDH 2004-X). Les informations relatives à la santé d'une personne constituent un élément important de sa vie privée (*Z c. Finlande*, 25 février 1997, § 71, Recueil des arrêts et décisions 1997-I). La Cour estime de plus que l'identité ethnique d'un individu doit aussi être considérée comme un élément important de sa vie privée (voir notamment l'article 6 de la Convention du Conseil de l'Europe de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« la Convention sur la protection des données »), cité au paragraphe 41 ci-dessus, qui fait entrer les données à caractère personnel révélant l'origine raciale, avec d'autres informations sensibles sur l'individu, parmi les catégories particulières de données ne pouvant être conservées que moyennant des garanties appropriées). L'article 8 de la Convention protège en outre un droit à l'épanouissement personnel et celui de nouer et de développer des relations avec ses semblables et le monde extérieur (voir, par exemple, *Burghartz*, précité, avis de la Commission, § 47, et *Friedl c. Autriche*, 31 janvier 1995, avis de la Commission, § 45, série A no 305-B). La notion de vie privée comprend par ailleurs des éléments se rapportant au droit à l'image (*Sciacca c. Italie*, no 50774/99, § 29, CEDH 2005-I).

67. Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 (*Leander c. Suède*, 26 mars 1987, § 48, série A no 116). Peu importe que les informations mémorisées soient ou non utilisées par la suite (*Amann c. Suisse [GC]*, no 27798/95, § 69, CEDH 2000-II). Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu l'un des aspects de la vie privée précités, la Cour tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés (voir, mutatis mutandis, *Friedl*, précité, avis de la Commission, §§ 49-51, et *Peck*, précité, § 59).

b. Application des principes précités au cas d'espèce

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

69. Les organes de la Convention se sont déjà penchés à diverses reprises, dans le contexte de procédures pénales, sur des questions se rapportant à la conservation par les autorités de telles données à caractère personnel. Pour ce qui est de la nature et de la portée des informations contenues dans chacune des trois catégories de données, la Cour a par le passé établi une distinction entre la conservation des empreintes digitales et celle des échantillons cellulaires et profils ADN au motif que les informations personnelles contenues dans ces deux dernières catégories se prêtent davantage à des utilisations ultérieures (*Van der Velden c. Pays-Bas (déc.)*, no 29514/05, CEDH 2006-XV). Elle estime en l'espèce que la question de l'atteinte au droit des requérants au respect de leur vie privée doit être examinée séparément pour la conservation de leurs échantillons cellulaires et profils ADN et pour celle de leurs empreintes digitales.

i. Les échantillons cellulaires et profils ADN

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

71. La Cour réaffirme son opinion selon laquelle les préoccupations d'un individu quant aux utilisations susceptibles d'être faites à l'avenir d'informations privées conservées par les autorités sont légitimes et pertinentes pour la question de savoir s'il y a eu ou non ingérence. De fait, compte tenu du rythme élevé auquel se succèdent les innovations dans le domaine de la génétique et des technologies de l'information, la Cour ne peut écarter la possibilité que les aspects de la vie privée se rattachant aux informations génétiques fassent à l'avenir l'objet d'atteintes par des voies nouvelles, que l'on ne peut prévoir aujourd'hui avec précision. Dès lors, la Cour n'aperçoit aucune raison justifiant qu'elle s'écarte de la conclusion à laquelle elle est parvenue dans l'affaire Van der Velden.

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

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

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

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

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

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

ii. Les empreintes digitales

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

79. C'est la Commission qui, dans l'affaire McVeigh et autres c. Royaume-Uni (nos 8022/77, 8025/77 et 8027/77, rapport de la Commission du 18 mars 1981, Décisions et rapports 25, p. 93, § 224), s'est penchée pour

la première fois sur la question du prélèvement et de la conservation d'empreintes digitales. Celles en cause dans ladite affaire avaient été prélevées dans le cadre d'une série de mesures d'enquête. La Commission admit que certaines de ces mesures au moins avaient porté atteinte au droit des requérants au respect de leur vie privée, mais elle ne trancha pas le point de savoir si la conservation des empreintes digitales aurait à elle seule été constitutive de pareille atteinte.

80. Dans l'affaire Kinnunen c. Finlande (no 24950/94, décision de la Commission du 15 mai 1996, non publiée), la Commission considéra que la conservation après l'arrestation du requérant de ses empreintes digitales et photographies ne s'analysait pas en une ingérence dans sa vie privée dès lors que ces éléments ne contenaient aucune appréciation subjective sujette à contestation. La Commission nota toutefois que les données en question avaient été détruites neuf ans plus tard à la demande du requérant.

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

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

83. Dans l'affaire P.G. et J.H. c. Royaume-Uni (no 44787/98, §§ 59-60, CEDH 2001-IX), la Cour a quant à elle estimé que l'enregistrement de données et le caractère systématique ou permanent de l'enregistrement était susceptible de faire entrer en jeu le droit au respect de la vie privée même si les données concernées étaient dans le domaine public ou disponibles d'une autre manière. Elle a observé que l'enregistrement de la voix d'une personne sur un support permanent en vue d'une analyse ultérieure était manifestement de nature, combiné à d'autres données personnelles, à faciliter l'identification de cette personne. Elle a donc jugé que l'enregistrement des voix des requérants en vue d'une telle analyse ultérieure avait porté atteinte à leur droit au respect de leur vie privée.

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

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

86. En l'espèce, la Cour note en outre que les empreintes digitales des requérants ont été relevées dans le cadre de procédures pénales pour être ensuite enregistrées dans une base de données nationale en vue de leur conservation permanente et de leur traitement régulier par des procédés automatisés à des fins d'identification criminelle. Chacun admet à cet égard que, de par les informations que les échantillons cellulaires et profils ADN contiennent, la conservation de ces éléments a un impact plus grand sur la vie privée que celle d'empreintes digitales. Toutefois, à l'instar de la baronne Hale of Richmond (paragraphe 25 ci-dessus), la Cour estime que, s'il peut se révéler nécessaire de distinguer entre les empreintes digitales, d'une part, et les échantillons et profils, d'autre part, pour ce qui est de leur prélèvement, de leur utilisation et de leur stockage lorsqu'il s'agit de trancher la question de la justification, il n'en demeure pas moins que la conservation d'empreintes digitales constitue une atteinte au droit au respect de la vie privée.

B. Justification de l'ingérence

1. Les arguments des parties

a. Les requérants

87. Les requérants soutiennent que la conservation des empreintes digitales, échantillons cellulaires et profils ADN ne se justifie pas au regard du second paragraphe de l'article 8. La législation interne conférerait aux autorités une très grande latitude pour utiliser les échantillons et profils ADN puisqu'elle prévoirait seulement que ceux-ci doivent être employés à des fins en rapport avec « la prévention ou la détection des infractions

pénales », « l'enquête sur une infraction » ou « la conduite de poursuites ». Ces objectifs seraient vagues et se prêteraient à des abus car ils risqueraient notamment de conduire à la collecte d'informations personnelles détaillées en dehors du cadre immédiat de l'enquête sur une infraction donnée. Les requérants estiment en outre que les garanties procédurales contre les usages impropres ou abusifs de ces informations sont insuffisantes. Les fichiers contenus dans l'ordinateur national de la police seraient accessibles non seulement à la police, mais aussi à cinquante-six organismes extérieurs à celle-ci, au nombre desquels figureraient des organismes publics et services administratifs, des groupes privés tels que British Telecom et l'association des assureurs britanniques, et même certains employeurs. De plus, cet ordinateur serait relié au système d'information Schengen, qui fonctionnerait à l'échelle européenne. En conséquence, leur affaire révélerait une atteinte très importante et critiquable au droit au respect de leur vie privée, comme en témoignerait notamment le débat public en cours au Royaume-Uni sur le sujet et les désaccords s'exprimant dans ce cadre. Au contraire de ce que plaide le Gouvernement, la question de la conservation de ces éléments serait de nature à faire naître de vives préoccupations chez les individus, et l'Etat ne disposerait que d'une marge d'appréciation étroite en la matière.

88. Pour les requérants, la conservation pendant une durée illimitée des empreintes digitales, échantillons cellulaires et profils ADN de personnes non condamnées ne peut passer pour « nécessaire dans une société démocratique » aux fins de la prévention des infractions pénales. En particulier, il n'y aurait absolument rien qui justifierait la conservation d'échantillons cellulaires une fois le profil ADN extrait. L'efficacité de la conservation des profils n'aurait pas non plus été démontrée de manière convaincante étant donné qu'il n'aurait pas été prouvé que le nombre élevé de concordances ADN mis en avant par le Gouvernement eût permis de condamner les coupables. De même, dans la plupart des exemples précis cités par le Gouvernement, ce ne serait pas la conservation des fiches qui aurait permis aux poursuites de déboucher sur des condamnations et, dans d'autres cas, les poursuites auraient aussi pu aboutir si la conservation des éléments en cause avait été plus limitée dans le temps et dans son ampleur.

89. Les requérants plaident en outre le caractère disproportionné de la conservation des éléments litigieux. Elle s'appliquerait de manière indifférenciée, sans limitation de durée, quelles que soient les infractions en cause et la situation des personnes concernées. Par ailleurs, la décision de conserver ou non les éléments en question ne serait ni prise ni contrôlée par un organe indépendant. Le régime de conservation serait de surcroît non conforme aux orientations définies par le Conseil de l'Europe dans ce domaine. Enfin, la conservation des fiches en question jetterait le doute sur des personnes ayant été acquittées ou ayant bénéficié d'un non-lieu, car cela laisserait entendre qu'elles n'étaient pas totalement innocentes. Cette mesure produirait donc une stigmatisation particulièrement préjudiciable aux enfants, tel M. S., et aux membres de certains groupes ethniques surreprésentés dans la base de données.

b. Le Gouvernement

90. Le Gouvernement considère qu'à supposer que la conservation des empreintes digitales, échantillons cellulaires et profils ADN des requérants soit constitutive d'une ingérence, celle-ci est justifiée au regard de l'article 8 § 2. D'abord, elle serait prévue par la loi, et plus précisément par l'article 64 de la loi de 1984, qui énoncerait de manière détaillée les pouvoirs et limitations en matière de prélèvement d'empreintes digitales et d'échantillons et indiquerait clairement que ces éléments sont conservés par les autorités quelle que soit l'issue de la procédure dans le cadre de laquelle ils ont été prélevés. En tout état de cause, l'exercice du pouvoir discrétionnaire de conserver des empreintes digitales et échantillons serait aussi soumis aux principes juridiques ordinaires régissant l'exercice de pouvoirs discrétionnaires et il serait susceptible de contrôle juridictionnel.

91. Par ailleurs, l'ingérence serait nécessaire et proportionnée aux buts légitimes que constituent la défense de l'ordre et la prévention des infractions pénales et/ou la protection des droits et libertés d'autrui. Il serait vital, pour la société en général, que les services chargés de faire respecter les lois puissent bénéficier au maximum des outils qu'offrent la technologie moderne et la criminalistique dans le cadre de la prévention et de la détection des infractions pénales et des enquêtes sur de telles infractions. Le Gouvernement plaide, statistiques à l'appui, que les éléments conservés représentent une valeur inestimable aux fins de la lutte contre la criminalité et le terrorisme et de la recherche des coupables. Il considère que les avantages que le système de la justice pénale retire de leur conservation sont immenses, les éléments en question permettant selon lui non seulement de trouver les coupables mais aussi de disculper les innocents et de prévenir et corriger les erreurs judiciaires.

92. Il indique qu'à la date du 30 septembre 2005, la base nationale de données ADN contenait 181 000 profils ADN d'individus qui auraient été en droit de faire effacer ces données avant l'adoption des amendements de 2001. Par la suite, 8 251 de ces profils auraient été reliés à des traces recueillies sur les lieux de 13 079 infractions, dont 109 meurtres, 55 tentatives de meurtre, 116 viols, 67 infractions sexuelles, 105 vols qualifiés et 126 cas de fourniture de substances illicites.

93. Le Gouvernement cite aussi en exemple dix-huit affaires où l'utilisation d'éléments ADN aurait permis à des enquêtes et poursuites d'aboutir à des condamnations. Dans dix d'entre elles, les profils ADN de suspects se seraient révélés correspondre à des traces relevées antérieurement sur les lieux d'infractions sans rapport avec

celles dont ils étaient soupçonnés et conservées dans la base de données, ce qui aurait permis de condamner les auteurs de ces infractions. Dans un autre cas, deux suspects arrêtés pour viol auraient pu être exclus du champ de l'enquête, leur profil ADN ne correspondant pas aux traces recueillies. Dans deux autres affaires, la conservation des profils ADN de personnes reconnues coupables de certaines infractions mineures (trouble à l'ordre public et vol) aurait permis d'établir leur participation à d'autres infractions commises plus tard. Dans un cas, la conservation du profil ADN d'un suspect à la suite d'une allégation d'infraction à la législation sur l'immigration aurait facilité son extradition vers le Royaume-Uni un an plus tard ; l'intéressé aurait alors été identifié comme étant un violeur et un meurtrier par l'une de ses victimes. Dans quatre cas, enfin, on aurait découvert jusqu'à deux ans après les faits que les profils ADN de quatre personnes soupçonnées d'avoir commis certaines infractions (détention d'armes offensives, trouble violent à l'ordre public et agression), mais non condamnées, correspondaient aux traces recueillies sur des victimes de viol.

94. Pour le Gouvernement, la conservation des empreintes digitales, échantillons cellulaires et profils ADN des requérants ne peut passer pour excessive, ces éléments ayant été stockés à des fins précises indiquées dans la loi, en toute sécurité et dans le respect des garanties prévues. La conservation n'aurait pas été motivée par la moindre raison de soupçonner les requérants d'avoir pris part à une infraction ou d'avoir une propension à commettre des infractions, et elle n'aurait pas non plus concerné des données se rapportant à des infractions présumées ayant déjà fait l'objet d'enquêtes par le passé. Les données conservées l'auraient été parce que la police les avait déjà légalement en sa possession et parce qu'elles pouvaient contribuer à l'avenir à la prévention et à la détection des infractions en général grâce à l'élargissement de la base de données. Pareille conservation ne provoquerait aucune stigmatisation et n'entraînerait aucune conséquence pratique pour les requérants, sauf si les éléments mémorisés venaient à correspondre à des profils tirés de traces recueillies sur les lieux d'infractions. Un juste équilibre aurait donc été ménagé, dans les limites de la marge d'appréciation de l'Etat, entre les droits de l'individu et l'intérêt général de la communauté.

2. L'appréciation de la Cour

a. Prévue par la loi

95. La Cour rappelle sa jurisprudence constante selon laquelle les termes « prévue par la loi » signifient que la mesure litigieuse doit avoir une base en droit interne et être compatible avec la prééminence du droit, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8. La loi doit ainsi être suffisamment accessible et prévisible, c'est-à-dire énoncée avec assez de précision pour permettre à l'individu – en s'entourant au besoin de conseils éclairés – de régler sa conduite. Pour que l'on puisse la juger conforme à ces exigences, elle doit fournir une protection adéquate contre l'arbitraire et, en conséquence, définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes (*Malone c. Royaume-Uni*, 2 août 1984, §§ 66-68, série A no 82, *Rotaru c. Roumanie* [GC], no 28341/95, § 55, CEDH 2000-V, et *Amann*, précité, § 56).

96. Le niveau de précision requis de la législation interne – laquelle ne peut du reste parer à toute éventualité – dépend dans une large mesure du contenu du texte considéré, du domaine qu'il est censé couvrir et du nombre et de la qualité de ses destinataires (*Hassan et Tchaouch c. Bulgarie* [GC], no 30985/96, § 84, CEDH 2000-XI, et références citées).

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

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

99. La Cour convient avec les requérants que le premier au moins de ces objectifs est exprimé en termes assez généraux et se prête à une interprétation très large. Elle rappelle que, dans ce contexte comme dans celui des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire (voir, *mutatis mutandis*, *Kruslin c. France*, 24 avril 1990, §§ 33 et 35, série A no 176-A, *Rotaru*, précité, §§ 57-59,

Weber et Saravia c. Allemagne (déc.), no 54934/00, CEDH 2006-XI, Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie, no 62540/00, §§ 75-77, 28 juin 2007, et Liberty et autres c. Royaume-Uni, no 58243/00, §§ 62-63, 1er juillet 2008). La Cour note cependant que ces aspects sont en l'espèce étroitement liés à la question plus large de la nécessité de l'ingérence dans une société démocratique. Compte tenu de l'analyse à laquelle elle s'est livrée aux paragraphes 105 à 126 ci-dessous, la Cour juge qu'il n'y a pas lieu de trancher le point de savoir si le libellé de l'article 64 répond aux exigences quant à la « qualité » de la loi, au sens de l'article 8 § 2 de la Convention.

b. But légitime

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

c. Nécessaire dans une société démocratique

i. Principes généraux

101. Une ingérence est considérée comme « nécessaire dans une société démocratique » pour atteindre un but légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants ». S'il appartient aux autorités nationales de juger les premières si toutes ces conditions se trouvent remplies, c'est à la Cour qu'il revient de trancher en définitive la question de la nécessité de l'ingérence au regard des exigences de la Convention (Coster c. Royaume-Uni [GC], no 24876/94, § 104, 18 janvier 2001, et références citées).

102. Il faut reconnaître à cet égard une certaine marge d'appréciation aux autorités nationales compétentes. Son étendue est variable et dépend d'un certain nombre de facteurs, dont la nature du droit en cause garanti par la Convention, son importance pour la personne concernée, la nature de l'ingérence et la finalité de celle-ci. Cette marge est d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre « intime » qui lui sont reconnus (Connors c. Royaume-Uni, no 66746/01, § 82, 27 mai 2004, et références citées). Lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, la marge d'appréciation laissée à l'Etat est restreinte (Evans c. Royaume-Uni [GC], no 6339/05, § 77, CEDH 2007-I). En revanche, elle est plus large 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 (Dickson c. Royaume-Uni [GC], no 44362/04, § 78, CEDH 2007-V).

103. La protection des données à 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 à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (voir, mutatis mutandis, Z c. Finlande, précité, § 95). La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (préambule et article 5 de la Convention sur la protection des données et principe 7 de la Recommandation no R (87) 15 du Comité des Ministres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police). Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (voir notamment l'article 7 de la Convention sur la protection des données). Les considérations qui précèdent valent tout spécialement lorsqu'est en jeu la protection de catégories particulières de données plus sensibles (article 6 de la Convention sur la protection des données), notamment des données ADN, qui, dans la mesure où elles contiennent le patrimoine génétique de la personne, revêtent une grande importance tant pour elle-même que pour sa famille (Recommandation no R (92) 1 du Comité des Ministres du Conseil de l'Europe sur l'utilisation des analyses de l'ADN dans le cadre du système de justice pénale).

104. L'intérêt des personnes concernées et de la collectivité dans son ensemble à voir protéger les données à caractère personnel, et notamment les données relatives aux empreintes digitales et génétiques, peut s'effacer devant l'intérêt légitime que constitue la prévention des infractions pénales (article 9 de la Convention sur la protection des données). Cependant, compte tenu du caractère intrinsèquement privé de ces informations, la

Cour se doit de procéder à un examen rigoureux de toute mesure prise par un Etat pour autoriser leur conservation et leur utilisation par les autorités sans le consentement de la personne concernée (voir, mutatis mutandis, Z c. Finlande, précité, § 96).

ii. Application de ces principes au cas d'espèce

105. Pour la Cour, il est hors de doute que la lutte contre la criminalité, et notamment contre le crime organisé et le terrorisme, qui constitue l'un des défis auxquels les sociétés européennes doivent faire face à l'heure actuelle, dépend dans une large mesure de l'utilisation des techniques scientifiques modernes d'enquête et d'identification. Le Conseil de l'Europe a reconnu il y a plus de quinze ans que les techniques d'analyse de l'ADN présentaient des avantages pour le système de la justice pénale (Recommandation no R (92) 1 du Comité des Ministres du Conseil de l'Europe, paragraphes 43-44 ci-dessus). Il est constant, par ailleurs, que les Etats membres ont réalisé depuis des progrès rapides et substantiels en matière d'utilisation des données ADN pour établir l'innocence ou la culpabilité d'une personne.

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

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

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

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

110. Cette situation est conforme à la Recommandation no R (92) 1 du Comité des Ministres du Conseil de l'Europe, qui insiste sur la nécessité d'établir des distinctions entre les différents types de cas et d'appliquer des durées précises de conservation des données, même dans les cas les plus graves (paragraphes 43-44 ci-dessus). En réalité, l'Angleterre, le pays de Galles et l'Irlande du Nord sont les seuls ordres juridiques au sein du Conseil de l'Europe à autoriser la conservation illimitée des empreintes digitales et des échantillons et profils ADN de toute personne, quel que soit son âge, soupçonnée d'avoir commis une infraction emportant inscription dans les fichiers de la police.

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

112. La Cour ne peut toutefois ignorer le fait que, en dépit des avantages susceptibles de découler d'un élargissement maximal de la base de données ADN, d'autres Etats contractants ont décidé de fixer des limites à la conservation et à l'utilisation de telles données afin de parvenir à un équilibre adéquat avec l'intérêt concurrent que constitue la préservation de la vie privée. Elle observe que la protection offerte par l'article 8 de la Convention serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part. Pour la Cour, le fort consensus qui existe à cet égard au sein des Etats

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

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

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

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

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

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

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

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

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

121. Le Gouvernement plaide que la conservation ne pourrait avoir un effet direct ou important sur les requérants que si des correspondances établies avec la base de données venaient à l'avenir à révéler leur implication dans des infractions. La Cour ne peut souscrire à cet argument. Elle réaffirme que le simple fait de

la conservation ou de la mémorisation de données à caractère personnel par les autorités publiques, quelle que soit la manière dont celles-ci ont été obtenues, doit passer pour emporter des conséquences directes sur la vie privée de l'individu concerné, que ces données soient utilisées par la suite ou non (paragraphe 67 ci-dessus).

122. Particulièrement préoccupant en l'occurrence est le risque de stigmatisation, qui découle du fait que les personnes dans la situation des requérants, qui n'ont été reconnus coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence, sont traitées de la même manière que des condamnés. Il convient de ne pas perdre de vue à cet égard que le droit de toute personne à être présumée innocente que garantit la Convention comporte une règle générale en vertu de laquelle on ne peut plus exprimer de soupçons sur l'innocence d'un accusé une fois que celui-ci a été acquitté (*Rushiti c. Autriche*, no 28389/95, § 31, 21 mars 2000, et références citées). Certes, la conservation de données privées concernant les requérants n'équivaut pas à l'expression de soupçons. Néanmoins, l'impression qu'ont les intéressés de ne pas être considérés comme innocents se trouve renforcée par le fait que les données les concernant sont conservées indéfiniment tout comme celles relatives à des personnes condamnées, alors que celles concernant des individus n'ayant jamais été soupçonnés d'une infraction doivent être détruites.

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

124. La Cour estime en outre que la conservation de données relatives à des personnes non condamnées peut être particulièrement préjudiciable dans le cas de mineurs, tel le premier requérant, en raison de leur situation spéciale et de l'importance que revêt leur développement et leur intégration dans la société. La Cour a déjà insisté, en s'inspirant des dispositions de l'article 40 de la Convention des Nations unies de 1989 relative aux droits de l'enfant, sur la place particulière qu'occupent les jeunes gens dans le domaine de la justice pénale, et elle a notamment souligné la nécessité de protéger leur vie privée dans le contexte des procédures pénales (*T. c. Royaume-Uni [GC]*, no 24724/94, §§ 75 et 85, 16 décembre 1999). De la même manière, la Cour considère qu'il faut veiller avec un soin particulier à protéger les mineurs de tout préjudice qui pourrait résulter de la conservation par les autorités, après un acquittement, des données privées les concernant. La Cour partage l'avis du Nuffield Council on Bioethics quant aux conséquences pour les jeunes gens d'une conservation illimitée de leurs échantillons et profils ADN et prend note des préoccupations exprimées par cet organisme au sujet de la surreprésentation dans la base de données des mineurs et des membres de minorités ethniques n'ayant été reconnus coupables d'aucune infraction à laquelle les politiques suivies auraient conduit (paragraphe 38-40 ci-dessus).

125. En conclusion, la Cour estime que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'Etat défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique. Cette conclusion dispense la Cour d'examiner les critiques formulées par les requérants à l'encontre de certains points précis du régime de conservation des données litigieuses, tels l'accès, trop large selon eux, à ces données et la protection, insuffisante à leurs yeux, offerte contre les usages impropres ou abusifs de ces données.

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

- **CEDH, 17 décembre 2009, M. B. c. France, n° 22115/06**

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

41. Le requérant invoque aussi la violation de l'article 8 qui dispose :

« 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. »

A. Thèses des parties

42. Le Gouvernement souligne que la contrainte résultant pour le requérant de son inscription au FIJAIS ne saurait s'analyser en une ingérence dans sa vie privée et familiale puisqu'elle se limite aux exigences prévues à l'article 706-53-5 du CPP (voir paragraphe 11 ci-dessus).

43. Il soutient que la mesure en cause a bien une base légale, la loi du 9 mars 2004 qui envisage les conséquences de l'inscription au FIJAIS pour les personnes concernées. Elle a pour but la défense de l'ordre et la prévention des infractions pénales, en particulier sur les mineurs (voir article 706-53-1 du CPP ci-dessus).

44. Enfin, le Gouvernement propose de mettre en balance l'intérêt pour la société de prévenir les infractions sexuelles et la gravité de l'atteinte au droit du requérant au respect de sa vie privée. Selon lui, la création du FIJAIS s'inscrit dans le cadre de la mise en place progressive d'un régime juridique propre aux infractions de nature sexuelle, qui trouve sa justification dans la prise de conscience relativement récente de la spécificité de ces infractions. Celle-ci résulte, d'une part, du fait que leurs auteurs sont souvent atteints de troubles de la personnalité, réel facteur de récidive, d'autre part de la souffrance particulière que ces infractions occasionnent aux victimes, particulièrement lorsqu'elles sont mineures au moment des faits. Ainsi, les autorités nationales ont mis en œuvre des mesures répressives et des mesures préventives. La création du FIJAIS, dans ce contexte, avait pour but de combler les lacunes du dispositif de prévention, dans les cas particulièrement graves d'infractions sexuelles. Le Gouvernement ajoute qu'il ressort de la jurisprudence de la Cour que celle-ci ne conteste pas aux Etats le droit, pour prévenir des infractions, de recueillir et de mémoriser dans des fichiers des renseignements sur des personnes pourvu que « des garanties adéquates et suffisantes [existent] contre les abus » (Leander c. Suède, 26 mars 1987, § 60, série A no 116).

45. En l'espèce, le requérant aurait bénéficié de toutes les garanties offertes par la loi. Il a été informé de son inscription par l'autorité judiciaire, le contrôle du fichier étant confié à un magistrat. Seuls sont concernés les auteurs d'infractions sexuelles graves mentionnées à l'article 706-47 du code précité et seules celles-ci autorisent un enregistrement automatique.

46. Quant aux autres garanties prévues par la loi, le Gouvernement rappelle que la durée de conservation des informations dépend de la gravité des infractions concernées : vingt ou trente ans. Il s'agit d'une durée maximale et les personnes concernées ont la possibilité de demander l'effacement du FIJAIS avant l'issue de ce délai. Cette demande peut être portée devant trois autorités : le procureur de la République, le juge des libertés et de la détention et le président de la chambre de l'instruction. Ce triple accès constitue, selon le Gouvernement, une triple garantie. En l'espèce, la mention de la condamnation au casier judiciaire du requérant rend irrecevable sa demande d'effacement du FIJAIS. Il dispose toutefois de la possibilité de demander sa réhabilitation judiciaire qui peut permettre de faire disparaître la condamnation du casier judiciaire. Par ailleurs, le FIJAIS est exclusivement accessible à certaines autorités, astreintes à une obligation de confidentialité, et dans des circonstances précisément déterminées par la loi. Enfin aucun rapprochement ne peut être effectué entre le FIJAIS et d'autres fichiers.

47. Le Gouvernement conclut que les garanties entourant l'inscription au FIJAIS sont telles qu'elles constituent une ingérence nécessaire dans une société démocratique au sens de l'article 8 § 2 de la Convention.

48. Le requérant considère que son inscription au FIJAIS, les contraintes qui en découlent et la durée d'inscription sont une atteinte grave à ses libertés individuelles.

B. Appréciation de la Cour

49. La Cour relève que le FIJAIS contient des données relatives à la vie privée du requérant. Ce fichier dépend du ministère de la Justice et est placé sous le contrôle du magistrat qui dirige le casier judiciaire. La Cour souligne qu'il ne lui appartient pas de spéculer sur le caractère sensible ou non des éléments recueillis ni sur les éventuels inconvénients subis par le requérant. Selon sa jurisprudence, la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu (*mutatis mutandis*, Leander, précité, § 48, et Kopp c. Suisse, 25 mars 1998, § 53, Recueil des arrêts et décisions 1998-II). Plus précisément, la Cour a déjà jugé que l'obligation - pour les personnes ayant fait l'objet d'une condamnation pour infraction sexuelle - d'indiquer à la police leur nom, date de naissance, adresse ou changement d'adresse relève de l'article 8 § 1 de la Convention (Adamson, précitée).

50. La Cour observe que les parties ne contestent pas que l'ingérence litigieuse était prévue par la loi et qu'elle poursuivait les buts légitimes de défense de l'ordre public et de prévention des infractions pénales (ibidem). Il lui faut donc examiner la nécessité de l'ingérence au regard des exigences de la Convention.
51. Il appartient aux autorités nationales de dire les premières où se situe le juste équilibre à ménager dans un cas donné avant que la Cour ne procède à une évaluation en dernier ressort, et une certaine marge d'appréciation est donc laissée en principe aux Etats dans ce cadre. L'ampleur de cette marge varie et dépend d'un certain nombre d'éléments, notamment de la nature des activités en jeu et des buts des restrictions (Smith et Grady c. Royaume-Uni, nos 33985/96 et 33986/96, § 88, CEDH 1999-VI).
52. Dès lors, lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, la marge d'appréciation laissée à l'Etat est en général restreinte.
53. La protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues par cet article (mutatis mutandis, Z c. Finlande, 25 février 1997, § 95, Recueil 1997-I). A l'instar de ce qu'elle a décidé dans l'arrêt S. et Marper c. Royaume-Uni ([GC], nos 30562/04 et 30566/04, § 103), 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 sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (voir paragraphes 21 et 22, notamment le préambule et l'article 5 de la Convention sur la protection des données et le principe 7 de la recommandation R (87) 15 du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police). Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (voir notamment l'article 7 de la Convention précitée).
54. La Cour ne saurait mettre en doute les objectifs de prévention d'un fichier tel que celui sur lequel est inscrit le requérant, condamné à cinq ans d'emprisonnement pour viol commis sur mineur. Le but de ce fichier, elle l'a déjà rappelé, vise à prévenir les infractions pénales, et à lutter contre la récidive en particulier, et en pareil cas, à faciliter l'identification de leurs auteurs. Les sévices sexuels constituent incontestablement un type odieux de méfaits qui fragilisent les victimes. Les enfants et autres personnes vulnérables ont droit à la protection de l'Etat, sous la forme d'une prévention efficace les mettant à l'abri de formes aussi graves d'ingérence dans des aspects essentiels de leur vie privée (Stubbing et autres c. Royaume-Uni, 22 octobre 1996, § 64, Recueil 1996-IV).
55. En même temps, les politiques pénales en Europe évoluent et accordent, à côté de la répression, une importance croissante à l'objectif de réinsertion de la détention, en particulier vers la fin d'une longue peine d'emprisonnement (Dickson c. Royaume-Uni [GC], no 44362/04, § 75, CEDH 2007-XIII). Une réinsertion réussie présume notamment la prévention de la récidive (voir le rapport du commissaire des droits de l'homme du Conseil de l'Europe cité dans l'arrêt Léger c. France, no 19324/02, § 49).
56. En l'espèce, le requérant fut inscrit automatiquement sur le fichier en vertu des dispositions transitoires de la loi du 9 mars 2004 (voir paragraphe 10 ci-dessus) et compte tenu du crime pour lequel il a été définitivement condamné. Cette inscription lui fut notifiée et il prit connaissance des obligations à sa charge.
57. S'agissant de ses obligations de justifier son adresse une fois par an et ses changements d'adresse sous peine d'un emprisonnement et d'une amende, la Cour a déjà jugé que cela n'était pas contraire aux principes de l'article 8 de la Convention (Adamson, précitée).
58. Quant à la durée de conservation des informations, la Cour constate qu'elle est de vingt ou trente ans selon la gravité de la condamnation entraînant l'inscription au FIJAIS.
59. Comme l'indique le Gouvernement, il s'agit d'une durée maximale. Quoi qu'importante en l'espèce puisqu'elle est de vingt ans, la Cour observe que l'effacement des données est de droit, une fois ce délai écoulé, lequel se compute dès que la décision ayant entraîné l'inscription cesse de produire tous ses effets. La Cour relève également que la personne concernée peut présenter une demande d'effacement au procureur de la République si la conservation des données la concernant n'apparaît plus pertinente compte tenu de la finalité du fichier, au regard de la nature de l'infraction, de l'âge de la personne lors de sa commission, du temps écoulé depuis lors et de sa personnalité actuelle (article 706-53-10 du CPP). La décision du procureur est susceptible de recours devant le juge des libertés et de la détention puis devant le président de la chambre de l'instruction.
60. La Cour considère que cette procédure judiciaire d'effacement des données assure un contrôle indépendant de la justification de la conservation des informations sur la base de critères précis (S. et Marper, précité, § 119) et présente des garanties suffisantes et adéquates du respect de la vie privée au regard de la gravité des

infractions justifiant l'inscription sur le fichier. Certes, la mémorisation des données pour une période aussi longue pourrait poser un problème sous l'angle de l'article 8 de la Convention, mais la Cour constate que le requérant a, en tout état de cause, la possibilité concrète de présenter une requête en effacement des données mémorisées alors que la décision ayant entraîné son inscription a cessé de produire tous ses effets. Dans ces conditions, la Cour est d'avis que la durée de conservation des données n'est pas disproportionnée au regard du but poursuivi par la mémorisation des informations.

61. Concernant les modalités d'utilisation du fichier et le champ des autorités publiques ayant accès à ce fichier, la Cour constate qu'il a été élargi à plusieurs reprises et qu'il ne se limite plus aux autorités judiciaires et de police mais que désormais des organes administratifs y ont aussi accès (article 706-53-7 du CPP, paragraphe 11 ci-dessus). Force est de constater que la consultation est exclusivement accessible à des autorités astreintes à une obligation de confidentialité et dans des circonstances précisément déterminées. De plus, la présente espèce ne prête pas à un examen *in concreto* de la question de l'ouverture de l'interrogation du fichier à des fins administratives.

62. En conclusion, la Cour estime que l'inscription au FIJAIS, telle qu'elle a été appliquée au requérant en l'espèce, traduit un juste équilibre entre les intérêts privés et publics concurrents en jeu, et que l'Etat défendeur n'a pas outrepassé sa marge d'appréciation acceptable en la matière. Partant, il n'y a pas eu, en l'espèce, violation de l'article 8 de la Convention.

- **CEDH, 18 avril 2013, M. K. c. France, n° 19522/09**

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.

B. Sur le fond

1. Arguments des parties

23. Le requérant ne conteste pas la légalité de l'ingérence dans son droit au respect de sa vie privée, mais il l'estime injustifiée. Il dénonce tout d'abord un manque de proportionnalité des moyens employés pour atteindre son but. Il estime que les dispositions de l'article 1er du décret de 1987, relatives au but de la mesure, sont trop étendues dans leur objet et vagues dans leur définition. Partant, les autorités disposent d'une latitude excessive, avec un pouvoir de conservation général et indifférencié. Il dénonce un risque d'abus réel au regard de la déviance affectant d'autres fichiers.

24. Par ailleurs, le requérant estime que la durée de conservation a été fixée arbitrairement et qu'elle équivaut à une absence de limitation dans le temps. A ses yeux, la durée de vingt-cinq ans correspond en réalité non pas à un maximum, mais à une norme, ce dont atteste le rejet lapidaire de sa demande devant les juges internes. Quant à la motivation du refus d'effacement, elle n'est pas encadrée et peut refléter un préjugé à l'égard du demandeur, comme en l'espèce.

25. Le requérant critique en outre une absence de garanties procédurales effectives, en soutenant que les juges peuvent non seulement remettre en cause l'autorité de la chose jugée au pénal pour refuser l'effacement, comme ce fut le cas pour lui, mais qu'en outre l'existence même des données dans le fichier entraîne, en soi, des remises en cause de la présomption d'innocence.

26. Le Gouvernement ne conteste pas que la conservation des données concernant le requérant au fichier automatisé des empreintes digitales (« FAED ») constitue une ingérence dans son droit au respect de sa vie privée.

27. Il estime cependant, d'une part, qu'elle était prévue par la loi, à savoir par l'article 55-1 du code de procédure pénale et le décret no 87-249 du 8 avril 1987 modifié, et, d'autre part, qu'elle poursuivait un but légitime de défense de l'ordre public, puisqu'elle a pour objet de déterminer les auteurs d'infractions pénales et de les poursuivre.

28. Le Gouvernement considère en outre que l'ingérence était nécessaire dans une société démocratique. Tout en rappelant que la jurisprudence de la Cour n'interdit pas aux Etats de recueillir et de mémoriser des données personnelles, dès lors qu'il existe des garanties adéquates et suffisantes, il insiste sur trois points : les Etats jouissent d'une certaine marge d'appréciation en la matière et celle-ci devrait être plus vaste s'agissant de simples empreintes digitales ; le FAED contribue grandement à la réussite des enquêtes et à la détection des usurpations d'identité ; de nombreuses garanties entourent la gestion du FAED. Concernant ces garanties, le Gouvernement précise que les données inscrites sont limitativement énumérées et que le fichier ne peut être consulté qu'à partir de la comparaison d'empreintes (et non à partir d'un nom ou d'une adresse). De plus, seuls des fonctionnaires de police et de gendarmerie habilités peuvent le consulter. Le traitement des données est placé sous le contrôle à la fois du procureur général près la cour d'appel et de la Commission nationale de l'informatique et des libertés (« CNIL »), qui est une autorité administrative indépendante. Tout en limitant la durée de conservation des données à vingt-cinq ans, le décret prévoit que l'intéressé peut en demander l'effacement, une action judiciaire étant disponible en cas de refus opposé par le procureur de la République. En l'espèce, le Gouvernement note que le requérant a fait usage de ce recours, en saisissant le juge des libertés et de la détention, puis le premier président de la cour d'appel. Il soutient par ailleurs que la Cour de cassation a examiné le pourvoi du requérant au regard des droits de la défense, bien qu'elle l'ait déclaré irrecevable.

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 no 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], no 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 no 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], no 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, no 16428/05, B.B. c. France, no 5335/06, et M.B. c. France, no 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 no 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, no 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], no 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], no 44362/04, § 78, CEDH 2007-XIII).

35. La protection des données à 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 à 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, no 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, 2o 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.

- **CEDH, 18 septembre 2014, *Brunet c/ France*, n° 21010/10**

1. L'existence de l'ingérence

1. La Cour constate d'emblée que l'inscription au STIC des données relatives au requérant a constitué une ingérence dans son droit à la vie privée, ce qui n'est pas contesté par le Gouvernement.

2. Justification de l'ingérence

a) Base légale et but légitime

2. La Cour observe que cette ingérence était « prévue par la loi » et qu'elle poursuivait les « buts légitimes » de défense de l'ordre, de prévention des infractions pénales, et de protection des droits d'autrui.

b) Nécessité de l'ingérence

i. Les principes généraux

3. Il lui reste donc à examiner la nécessité de l'ingérence au regard des exigences de la Convention, qui commandent 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 » (voir, notamment, *M.K. c. France*, n° 19522/09, § 33, 18 avril 2013).

4. 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 c. Royaume-Uni* [GC], n°s 30562/04 et 30566/04, § 101, CEDH 2008). 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, est donc laissée en principe aux États dans ce cadre (voir, notamment, *Klass et autres c. Allemagne*, 6 septembre 1978, § 49, série A n° 28, *Smith et Grady c. Royaume-Uni*, n°s 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). 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). En revanche, lorsqu'il n'y a pas de consensus au sein des États 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).

5. La protection des données à 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 à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. Cette nécessité 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 s'assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (*S. et Marper c. Royaume-Uni*, précité, § 103, *Gardel c. France*, précité, § 62, CEDH 2009, et *M.K. c. France*, précité, § 35).

6. Pour apprécier le caractère proportionné de la durée de conservation des informations au regard du but poursuivi par leur mémorisation, la Cour tient compte de l'existence ou non d'un contrôle indépendant de la justification de leur maintien dans le système de traitement, exercé sur la base de critères précis tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière (*S. et Marper c. Royaume-Uni*, précité, § 119, et *B.B. c. France*, précité, § 68).

7. 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. 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, et *M.K.*, précité, § 36).

ii. L'application des principes susmentionnés au cas d'espèce

8. La Cour observe d'emblée que le requérant se plaint d'une atteinte susceptible d'être portée à sa vie privée et familiale du fait de son inscription au fichier, dans le cadre d'une éventuelle procédure devant le juge aux affaires familiales relative au droit de garde de son enfant. Or, elle constate que ce magistrat ne figure pas parmi les personnes ayant accès au fichier concerné. La situation dénoncée par le requérant n'est donc pas susceptible de se produire.

9. En revanche, s'agissant du caractère outrageant invoqué, la Cour note que si les informations répertoriées au STIC ne comportent ni les empreintes digitales (à la différence du fichier automatisé des empreintes digitales – voir *M.K.*, précité) ni le profil ADN des personnes, elles présentent néanmoins un caractère intrusif non négligeable, en ce qu'elles font apparaître des éléments détaillés d'identité et de personnalité en lien avec des infractions constatées, dans un fichier destiné à la recherche des infractions.

10. En outre, la Cour relève que le requérant a bénéficié, à la suite de la médiation pénale, d'un classement sans suite justifiant qu'il reçoive un traitement différent de celui réservé à une personne condamnée, afin d'éviter tout risque de stigmatisation (*S. et Marper*, précité, § 22, et *M.K.*, précité, § 42). À ce titre, elle observe que depuis la loi du 14 mars 2011, l'article 230-8 du code de procédure pénale dispose que, dans une telle hypothèse, le classement sans suite doit faire l'objet d'une mention sur la fiche enregistrée au STIC et les données relatives à la personne concernée ne peuvent alors plus être consultées dans le cadre de certaines enquêtes administratives. En l'espèce, la Cour ignore si la décision du ministère public a été effectivement inscrite parmi les informations concernant le requérant. Néanmoins, elle constate qu'en tout état de cause cette mesure n'a pas d'effet sur la durée de conservation de la fiche, qui est de vingt ans. Or, elle considère que cette durée est importante, compte tenu de l'absence de déclaration judiciaire de culpabilité et du classement sans suite de la procédure après le succès de la médiation pénale. Il lui appartient donc de s'interroger sur le caractère proportionné d'un tel délai, en tenant compte de la possibilité pour l'intéressé de demander l'effacement anticipé des données (voir *mutatis mutandis*, *M.K.*, précité, § 45).

11. À cet égard, la Cour relève que la loi, dans sa version applicable à l'époque des faits comme dans celle en vigueur, ne donne au procureur le pouvoir d'ordonner l'effacement d'une fiche que dans l'hypothèse d'un non-

lieu ou d'un classement sans suite motivé par une insuffisance des charges, outre les cas de relaxe ou d'acquiescement pour lesquels l'effacement est de principe mais où il peut prescrire le maintien des données au STIC. En l'espèce, pour rejeter la demande présentée à cette fin par le requérant, le procureur de la République d'Evry a appliqué strictement ces dispositions et s'est borné à constater que la procédure concernée avait fait l'objet d'une décision de classement sans suite fondée sur une autre cause que l'absence d'infraction ou son caractère insuffisamment caractérisé. Il n'avait donc pas compétence pour vérifier la pertinence du maintien des informations concernées dans le STIC au regard de la finalité de ce fichier, ainsi que des éléments de fait et de personnalité. La Cour estime qu'un tel contrôle ne saurait passer pour effectif, l'autorité chargée de l'exercer n'ayant pas de marge d'appréciation pour évaluer l'opportunité de conserver les données.

12. De même, elle note qu'à l'époque des faits la décision du procureur de la République n'était susceptible d'aucun recours. Certes, d'une part, le droit interne permet désormais à l'intéressé d'adresser une nouvelle demande au magistrat référent visé à l'article 230-9 du code de procédure pénale, comme le soutient le Gouvernement. La Cour observe néanmoins que le texte précise que ce magistrat « dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles (...) que le procureur de la République ». Aux yeux de la Cour, un tel recours ne présente donc pas le caractère d'effectivité nécessaire, l'autorité décisionnaire ne disposant d'aucune marge d'appréciation quant à la pertinence du maintien des informations au fichier, notamment lorsque la procédure a été classée sans suite après une médiation pénale, comme en l'espèce. D'autre part, la jurisprudence récente du Conseil d'État reconnaît la possibilité d'exercer un recours pour excès de pouvoir contre les décisions du procureur en matière d'effacement ou de rectification, qui ont pour objet la tenue à jour du STIC et sont détachables d'une procédure judiciaire (paragraphe 19 ci-dessus). Cependant, la Cour constate que cette faculté n'était pas reconnue à l'époque des faits, le requérant s'étant vu expressément notifier l'absence de toute voie de contestation ouverte contre la décision du procureur du 1^{er} décembre 2009.

13. Ainsi, bien que la conservation des informations insérées dans le STIC soit limitée dans le temps, il en découle que le requérant n'a pas disposé d'une possibilité réelle de demander l'effacement des données le concernant et que, dans une hypothèse telle que celle de l'espèce, la durée de vingt ans prévue est en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum (*M.K.*, précité).

14. En conclusion, la Cour estime que l'État défendeur a outrepassé sa marge d'appréciation en la matière, le régime de conservation des fiches dans le STIC, tel qu'il a été appliqué au requérant, 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.

15. Il y a donc eu violation de l'article 8 de la Convention.

- **CEDH, 22 juin 2017, Aycaguer c. France, n° 8806/2**

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

19. Le requérant dénonce une atteinte à son droit au respect de sa vie privée, en raison de l'ordre qui lui a été fait de se soumettre à un prélèvement biologique en vue de son inscription au FNAEG et pour lequel son refus d'obtempérer a donné lieu à une condamnation pénale. Il invoque l'article 8 de la Convention, qui se lit comme suit :

« 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. »

20. Le Gouvernement s'oppose à cette thèse.

A. Sur la recevabilité

21. La Cour constate que la requête n'est pas manifestement mal fondée au sens de l'article 35 § 3 a) de la Convention et qu'elle ne se heurte par ailleurs à aucun autre motif d'irrecevabilité. Elle la déclare donc recevable.

B. Sur le fond

1. Arguments des parties

a) Le requérant

22. Le requérant note d'abord, alors que l'objet initial du FNAEG était de regrouper les empreintes génétiques des délinquants sexuels, que ce fichier concerne aujourd'hui un grand nombre d'infractions, quels que soient leur degré de gravité et l'importance de l'atteinte portée à l'ordre public. Selon lui, le fichage litigieux ne peut pas être considéré comme légitime pour toutes les infractions énumérées à l'article 706-55 du CPP, allant des crimes contre l'humanité aux actes commis dans le cadre de violences syndicales. Le caractère généralisé et indifférencié rendrait ce fichage contraire aux principes de l'article 8 de la Convention, dès lors qu'il n'est ni justifié au regard du but poursuivi ni nécessaire dans la mesure où il n'existe aucun pouvoir d'appréciation et aucune modulation en fonction de l'infraction commise.

23. Le requérant relève en outre que le Gouvernement n'explique pas en quoi le fichage de sa personne serait nécessaire durant quarante ans ou pourquoi il serait susceptible de récidiver. Compte tenu de la nature et du niveau de gravité de l'infraction pour laquelle il a été condamné, il est selon lui disproportionné de conserver son empreinte ADN pendant quarante ans.

24. Quant à la durée de conservation des données, le requérant considère également que si la période de quarante ans était conforme à la Constitution française, le Conseil constitutionnel n'aurait pas émis de réserves d'interprétation et le Gouvernement n'envisagerait pas de la modifier par un décret. Il note toutefois qu'à ce jour, aucune initiative n'a été prise par le Gouvernement dans ce sens. Il observe également que la durée de conservation des empreintes digitales pour des infractions parmi les plus graves (*Gardel c. France*, no 16428/05, § 67, CEDH 2009) est inférieure à celle prévue par le FNAEG.

25. Le requérant souligne en outre que le fichier est placé sous le contrôle d'un magistrat du parquet qui n'est pas une autorité judiciaire au sens de la Convention (*Moulin c. France*, no 37104/06, § 57, 23 novembre 2010). Ainsi, toute requête en effacement des données est à présenter à un magistrat dépourvu de garantie d'indépendance. De plus, le FNAEG poursuit des fins policières et il est consultable, sans véritables garanties pour les intéressés, par de nombreux organismes policiers internationaux.

b) Le Gouvernement

26. Le Gouvernement, qui ne conteste pas l'existence d'une ingérence dans le droit au respect de la vie privée du requérant, note d'abord que cette ingérence avait sa base légale dans l'article 706-56 du CPP, le régime juridique du FNAEG étant défini aux articles 706-54 et s. et R. 53-9 et s. dudit code.

27. Il indique que le FNAEG est destiné à faciliter l'identification et la recherche, à l'aide de leur profil génétique, des auteurs des infractions. L'importance que le législateur porte au développement de ce fichier et à son effectivité l'a conduit en 2001 à pénaliser le refus de se soumettre au prélèvement. L'ensemble du dispositif relatif au FNAEG a été validé par le Conseil constitutionnel (paragraphe 16 ci-dessus). Par ailleurs, le FNAEG est selon lui à rapprocher du fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS), que la Cour a reconnu compatible avec les exigences de l'article 8 de la Convention (*B.B. c. France*, no 5335/06, 17 décembre 2009, *M.B. c. France*, no 22115/06, 17 décembre 2009, et *Gardel*, précité). L'ingérence litigieuse poursuivait donc un but légitime consistant en la prévention des infractions pénales.

28. Le Gouvernement souligne qu'à la différence de la réglementation contestée dans l'affaire *S. et Marper* (précité, § 119), seules les infractions qui sont limitativement énumérées dans l'article 706-55 du CPP donnent lieu à une inscription au FNAEG. Si le fichier a été initialement destiné à recevoir les empreintes génétiques dans le seul cadre de la délinquance sexuelle, son champ d'application a été étendu par plusieurs réformes successives. Les infractions visées présentent un certain degré de gravité et sont, sauf une, passibles d'une peine de prison. À l'exception des crimes et délits punis de dix ans d'emprisonnement, le prélèvement ne peut être effectué sans l'accord de la personne concernée et il est impossible de procéder, à partir des empreintes génétiques conservées, à un examen des caractéristiques génétiques.

29. Le Gouvernement relève en outre que le procureur de la République n'a pas le pouvoir d'apprécier l'opportunité d'inscrire ou non au FNAEG une personne condamnée pour l'une des infractions concernées. En effet, l'emploi de l'indicatif à l'article R. 53-21 du CPP ne laisse aucune marge d'appréciation aux procureurs.

30. De l'avis du Gouvernement, d'importantes garanties procédurales entourent les conditions d'utilisation, de consultation et de conservation des données au FNAEG. Ce fichier est mis en œuvre par la direction centrale de la police judiciaire du ministère de l'Intérieur et placé sous le double contrôle d'un magistrat du parquet hors hiérarchie, nommé par arrêté du Garde des Sceaux, et de la commission nationale de l'informatique et des libertés. L'accès aux informations et la possibilité de procéder à des opérations de rapprochement n'est possible qu'aux personnels de la sous-direction de la police scientifique et technique, ainsi qu'à ceux de la gendarmerie dûment habilités.

31. Le Gouvernement estime ensuite que l'absence de procédure d'effacement pour les personnes condamnées n'apparaît pas excessive, la durée de conservation maximale étant limitée à quarante ans, l'inscription du profil génétique au FNAEG n'impliquant aucune obligation positive pour la personne concernée et les données n'étant utilisées qu'en cas de commission de nouveaux faits.

32. Néanmoins, compte tenu des réserves formulées par le Conseil constitutionnel, dont l'une porte sur la proportionnalité de la durée de conservation des profils génétiques, et afin de s'y conformer, le Gouvernement indique qu'il s'apprête à soumettre au Conseil d'État un projet de décret destiné à modifier en conséquence les dispositions de l'article R. 53-14 du CPP.

2. Appréciation de la Cour

33. La Cour rappelle que le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 (Leander c. Suède, 26 mars 1987, § 48, série A no 116). Peu importe que les informations mémorisées soient ou non utilisées par la suite (Amann c. Suisse [GC], no 27798/95, § 69, CEDH 2000-II). Quant aux profils ADN, ils contiennent une quantité importante de données à caractère personnel uniques (S. et Marper, précité, § 75).

34. Par ailleurs, la Cour précise d'emblée qu'elle a pleinement conscience que, pour protéger leur population comme elles en ont le devoir, les autorités nationales sont amenées à constituer des fichiers contribuant efficacement à la répression et à la prévention de certaines infractions, notamment les plus graves, comme celles de nature sexuelle pour lesquelles le FNAEG a été créé (cf., notamment, Gardel, B.B. et M.B., précités, respectivement §§ 63, 62 et 54). Toutefois, de tels dispositifs ne sauraient être mis en œuvre dans une logique excessive de maximalisation des informations qui y sont placées et de la durée de leur conservation. En effet, sans le respect d'une nécessaire proportionnalité au regard des objectifs légitimes qui leur sont attribués, les avantages qu'ils apportent seraient obérés par les atteintes graves qu'ils causeraient aux droits et libertés que les États doivent assurer en vertu de la Convention aux personnes placées sous leur juridiction (M.K. c France, no 19522/09, § 35, 18 avril 2013).

35. En l'espèce, elle constate que le requérant n'est pas, à ce jour, inscrit sur le FNAEG, puisqu'il a refusé de se soumettre au prélèvement de son ADN imposé par la loi. Il a toutefois fait l'objet d'une condamnation pénale à ce titre. Il n'est pas sujet à controverse que cette condamnation s'analyse en une ingérence dans le droit du requérant au respect de sa vie privée au sens de l'article 8 § 1 de la Convention.

36. La Cour observe également que les parties ne contestent pas que l'ingérence litigieuse était prévue par la loi, à savoir les articles 706-54 à 706-56 et R. 53-9 et s. du CPP, et qu'elle poursuivait le but légitime de détection et, par voie de conséquence, de prévention des infractions pénales.

37. Il incombe donc à la Cour d'examiner la nécessité de cette ingérence au regard des exigences de la Convention. Il appartient aux autorités nationales de dire les premières où se situe le juste équilibre à ménager dans un cas donné avant que la Cour ne procède à une évaluation en dernier ressort, et une certaine marge d'appréciation est donc laissée en principe aux États dans ce cadre. L'ampleur de cette marge varie et dépend d'un certain nombre d'éléments, notamment de la nature des activités en jeu et des buts des restrictions. Lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, la marge d'appréciation laissée à l'État est en général restreinte.

38. La protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues par cet article. La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (B.B., précité, § 61), tout en offrant une possibilité concrète de présenter une requête en effacement des données mémorisées (B.B. c France, précité, § 68, et Brunet, précité, §§ 41-43).

39. En l'espèce, l'inscription sur le fichier, évitée par le requérant au prix d'une condamnation pénale, n'emporte en elle-même aucune autre obligation à la charge de l'intéressé. De plus, elle obéit à des modalités de consultation suffisamment encadrées.

40. La Cour constate également que l'article 706-56 du CPP précise qu'elle peut être réalisée à partir de matériel biologique qui se serait naturellement détaché du corps de l'intéressé (paragraphe 14 ci-dessus).

41. Par ailleurs, en application de l'article 706-54 du CPP, elle note que seules les infractions limitativement énumérées par l'article 706-55 du CPP peuvent donner lieu à une inscription au FNAEG.

42. À cet égard, il convient cependant de noter qu'en vertu de l'article R. 53-14 du CPP, la durée de conservation des profils ADN ne peut dépasser quarante ans s'agissant des personnes condamnées pour l'une des infractions mentionnées à l'article 706-55, qui présenteraient toutes, selon le Gouvernement, « un certain degré de gravité ». La Cour relève tout d'abord qu'il s'agit en principe d'une période maximum qui aurait dû

être aménagée par décret. Or, ce dernier n'ayant pas vu le jour, la durée de quarante ans est en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum (M.K., précité, § 45, et Brunet, précité, § 43), et ce en particulier pour des personnes ayant atteint un certain âge.

43. La Cour observe ensuite que le Conseil constitutionnel a rendu, le 16 septembre 2010, une décision déclarant les dispositions relatives au fichier incriminé conformes à la Constitution, sous réserve entre autres « de proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées » (paragraphe 15 ci-dessus). À ce jour, cette réserve n'a pas reçu de suite appropriée (paragraphe 14 et 42 ci-dessus). Ainsi, la Cour relève qu'aucune différenciation n'est actuellement prévue en fonction de la nature et de la gravité de l'infraction commise, et ce nonobstant l'importante disparité des situations susceptibles de se présenter dans le champ d'application de l'article 706-55 du CPP. La situation du requérant en atteste, avec des agissements qui s'inscrivaient dans un contexte politique et syndical, concernant de simples coups de parapluie donnés en direction de gendarmes qui n'ont pas même été identifiés (paragraphe 7 et 8 ci-dessus), par comparaison avec la gravité des faits susceptibles de relever des infractions particulièrement graves visées par l'article 706-55 du CPP, à l'instar notamment des infractions sexuelles, du terrorisme ou encore des crimes contre l'humanité ou de la traite des êtres humains pour ne citer que ces exemples. En cela, la présente affaire se distingue clairement, en particulier, 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).

44. Par ailleurs, s'agissant de la procédure d'effacement, il n'est pas contesté que celle-ci n'existe que pour les personnes soupçonnées, et non pour celles qui ont été condamnées, à l'instar du requérant. Or, la Cour estime que les personnes condamnées devraient également se voir offrir une possibilité concrète de présenter une requête en effacement des données mémorisées (B.B. c France, précité, § 68, et Brunet, précité, §§ 41-43), et ce, comme elle l'a rappelé précédemment, afin que la durée de conservation soit proportionnée à la nature des infractions et aux buts des restrictions (paragraphe 37 ci-dessus ; cf., mutatis mutandis, Peruzzo et Martens c. Allemagne (déc.), nos 7841/08 et 57900/12, § 44, 6 juin 2013, ainsi que B.B. et M.B., précités, respectivement §§ 62 et 54).

45. Dès lors, la Cour estime que le régime actuel de conservation des profils ADN dans le FNAEG, auquel le requérant s'est opposé en refusant le prélèvement, n'offre pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante à l'intéressé. Elle ne traduit donc pas un juste équilibre entre les intérêts publics et privés concurrents en jeu.

46. Ces éléments suffisent à la Cour pour conclure que l'État défendeur a outrepassé sa marge d'appréciation en la matière. Dès lors, la condamnation pénale du requérant pour avoir refusé de se soumettre au prélèvement destiné à l'enregistrement de son profil dans le FNAEG s'analyse en une atteinte disproportionnée à son droit 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.

b. Jurisprudence administrative

- CE, 17 juillet 2013, n° 359417

1. Considérant que, pour confirmer le jugement en date du 31 mars 2011 par lequel le tribunal administratif de Paris a rejeté la demande de M. A...tendant à l'annulation de la décision en date du 3 décembre 2008 du procureur près le tribunal de grande instance de Paris refusant d'ordonner l'effacement des mentions le concernant dans le "système de traitement des infractions constatées" (STIC), ainsi que du courrier du ministre de l'intérieur, de l'outre mer et des collectivités territoriales du 10 février 2009 confirmant la décision du procureur, la cour administrative d'appel de Paris a jugé que les décisions du procureur de la République relatives à l'effacement de mentions figurant dans ce fichier constituent des mesures d'administration judiciaire et qu'en conséquence la demande de M. A... était portée devant un ordre de juridiction incompétent pour en connaître ;

2. Considérant qu'aux termes de l'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure, alors en vigueur : " I. Les services de la police nationale et de la gendarmerie nationale peuvent mettre en oeuvre des applications automatisées d'informations nominatives recueillies au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'Etat, afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs (...) / III. - Le

traitement des informations nominatives est opéré sous le contrôle du procureur de la République compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande. En cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention sauf si le procureur de la République ordonne l'effacement des données personnelles " ; que l'article 25 de la même loi, qui rétablit l'article 17-1 de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, définit les conditions et finalités de la consultation, dans le cadre d'enquêtes administratives préalables aux décisions administratives qu'il mentionne, des données nominatives recueillies dans ces fichiers ; que l'article 1er du décret du 5 juillet 2001 pris pour l'application des dispositions du troisième alinéa de l'article 31 de la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées, dans sa rédaction alors en vigueur, autorise le ministère de l'intérieur (direction générale de la police nationale) à " mettre en oeuvre une application automatisée d'informations nominatives dénommée " système de traitement des infractions constatées " (STIC) " ; qu'en application de l'article 2 de ce décret, les données à caractère personnel relatives aux personnes mises en cause ainsi que la qualification des faits, telles qu'elles sont enregistrées dans le STIC, sont transmises au procureur de la République territorialement compétent en même temps que la procédure ; qu'aux termes de l'article 3 de ce décret, " le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent conformément aux dispositions du III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure " ;

3. Considérant qu'il résulte de ces dispositions que, si les données nominatives figurant dans le " système de traitement des infractions constatées " portent sur des informations recueillies au cours d'enquêtes préliminaires ou de flagrante ou d'investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que certaines contraventions de cinquième classe, les décisions en matière d'effacement ou de rectification, qui ont pour objet la tenue à jour de ce fichier et sont détachables d'une procédure judiciaire, constituent des actes de gestion administrative du fichier et peuvent faire l'objet d'un recours pour excès de pouvoir devant le juge administratif ; qu'en jugeant que les décisions du procureur de la République relatives à l'effacement des mentions figurant dans le " système de traitement des infractions constatées " constituent des mesures d'administration judiciaire, la cour administrative d'appel de Paris a commis une erreur de droit ; que, dès lors et sans qu'il soit besoin d'examiner les autres moyens du pourvoi, son arrêt doit être annulé ;

4. Considérant qu'il y a lieu, dans les circonstances de l'espèce, de mettre à la charge de l'Etat la somme de 1500 euros à verser à M.A..., au titre des dispositions de l'article L 761-1 du code de justice administrative ;

- **CE, 11 avril 2014, n° 360759**

En ce qui concerne le droit d'opposition et de rectification :

17. Considérant, en premier lieu, que pour les motifs énoncés ci-dessus, la requérante en saurait utilement soutenir que le législateur aurait méconnu sa compétence en autorisant le pouvoir réglementaire, par l'article 38 de la loi du 6 janvier 1978, à écarter, comme en l'espèce, le droit d'opposition par une disposition expresse de l'acte autorisant le traitement ;

18. Considérant, en second lieu, qu'aux termes de l'article 230-8 du code de procédure pénale : " Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire (...) " ; que l'article 230-9 du même code prévoit qu'un magistrat, chargé de suivre la mise en oeuvre et la mise à jour du TAJ et désigné à cet effet par le ministre de la justice, concourt à l'application de l'article 230-8 et qu'il dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles dans le TAJ que le procureur de la République ; que l'un et l'autre ont un accès direct au traitement et doivent se prononcer, dans un délai d'un mois, sur les demandes de rectification ; que l'article 40-31 du code de procédure pénale issu du décret attaqué précise par ailleurs que de telles demandes peuvent indifféremment leur être adressées ou être adressées à la CNIL si elles sont formulées par des personnes physiques, mais qu'elles doivent être adressées au seul procureur de la République s'agissant des personnes morales ;

19. Considérant que si les données nominatives figurant dans le TAJ portent sur des informations recueillies au cours d'enquêtes préliminaires ou de flagrante ou d'investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que certaines contraventions de cinquième classe, les décisions en matière d'effacement ou de rectification prises par le procureur de la République ou par le magistrat mentionné à l'article 230-9 du code de procédure pénale, qui ont pour objet la tenue à jour de ce fichier et sont détachables d'une

procédure judiciaire, constituent non pas des mesures d'administration judiciaire, mais des actes de gestion administrative du fichier ; qu'elles peuvent par suite faire l'objet d'un recours pour excès de pouvoir devant le juge administratif ; qu'il suit de là que la requérante n'est pas fondée à soutenir que le décret attaqué méconnaîtrait le droit au recours effectif garanti par l'article 13 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, au motif que les décisions refusant de procéder à l'effacement ou à la rectification demandée ne seraient susceptibles de faire l'objet d'aucun recours ;

20. Considérant qu'il résulte de ce qui précède que la Ligue des droits de l'homme n'est pas fondée à demander l'annulation du décret qu'elle attaque ; que ses conclusions présentées au titre des dispositions de l'article L. 761-1 du code de justice administrative, ne peuvent, par suite, qu'être rejetées ;

- **CE, avis 30 mars 2016, n° 395119**

1. Aux termes de l'article 230-6 du code de procédure pénale qui autorise sa mise en oeuvre, le traitement des antécédents judiciaires a pour finalité de " faciliter la constatation des infractions à la loi pénale, le rassemblement de preuves de ces infractions et la recherche de leurs auteurs ". Il a également pour finalité, en application des articles L. 234-1 à L. 234-4 du code de la sécurité intérieure, " dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la Nation ", de contribuer à mettre en oeuvre des mesures de protection ou recueillir des renseignements pour la prise de décisions administratives relatives à des emplois ou activités mentionnés à l'article L. 114-1 du même code, par l'intermédiaire de consultations autorisées, ainsi que, en application de l'article 17-1 de la loi du 21 janvier 1995, de faciliter l'instruction des demandes en matière de nationalité, de titres de séjour et ordres nationaux.

2. Aux termes de l'article 230-7 du code de procédure pénale qui détermine les données qui peuvent être collectées par ce traitement, il peut contenir des informations sur les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission de certaines infractions mentionnées au 1° de l'article 230-6, sur les victimes de ces infractions et sur les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort. Aux termes du premier alinéa de l'article 230-8 du code de procédure pénale : " Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent qui demande qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. En cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquiescement ou de relaxe devenue définitive, il en avise la personne concernée. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Les autres décisions de classement sans suite font l'objet d'une mention. Lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1, L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. ". Le décret n° 2012-652 du 4 mai 2012, pris sur le fondement de ces dispositions, encadre la mise en oeuvre du traitement des antécédents judiciaires. L'article R. 40-27 du code de procédure pénale fixe la durée de conservation des données concernant les personnes mises en cause dans le cadre des procédures établies par les services chargés des opérations de police judiciaire. Cette durée est modulée en fonction de l'âge de la personne mise en cause, de la gravité des infractions et de l'inscription de nouveaux faits dans le fichier.

3. Il résulte de ces dispositions que le législateur a entendu décrire entièrement les possibilités de radiation, correction ou maintien de données dans le fichier " traitement des antécédents judiciaires ", offertes à l'autorité à laquelle il a confié la responsabilité de contrôler sa mise en oeuvre.

4. Il en découle, en premier lieu, que saisis d'une demande d'effacement de données qui ne sont pas au nombre de celles que l'article 230-7 du code de procédure pénale autorise à collecter dans le traitement des antécédents judiciaires, le procureur de la République ou le magistrat référent mentionné à l'article 230-9 du même code, désignés par la loi pour contrôler le fichier, sont tenus d'en ordonner l'effacement.

5. En deuxième lieu, les dispositions de l'article 230-8 du code de procédure pénale citées au point 2 ne prévoyant de règles particulières relatives au maintien ou à l'effacement des données du traitement des antécédents judiciaires qu'en cas de décisions de relaxe, d'acquiescement, de non-lieu ou de classement sans suite,

le législateur doit être regardé comme n'ayant entendu ouvrir la possibilité d'effacement que dans les cas où les poursuites pénales sont, pour quelque motif que ce soit, demeurées sans suite. Hors cette hypothèse, les données ne peuvent être effacées qu'à l'issue de la durée de conservation fixée par voie réglementaire et le procureur de la République ne peut alors que refuser une demande d'effacement avant ce terme.

6. En troisième lieu, si la procédure a abouti à une décision de relaxe ou d'acquiescement, le principe est l'effacement des données et l'exception, le maintien pour des raisons tenant à la finalité du fichier. Lorsque les faits à l'origine de l'enregistrement des données dont l'effacement est demandé ont fait l'objet d'une ordonnance de non-lieu rendue par le juge d'instruction en application de l'article 177 du code de procédure pénale ou d'un classement sans suite pour insuffisance de charges par le procureur de la République, les données sont conservées dans le fichier mais sont assorties d'une mention qui fait obstacle à la consultation dans le cadre des enquêtes administratives. Le procureur de la République a toutefois la possibilité d'ordonner leur effacement. Lorsque les faits à l'origine de l'enregistrement des données dont l'effacement est demandé ont fait l'objet d'un classement sans suite pour un autre motif que l'insuffisance de charges, les données sont assorties d'une mention et les dispositions précitées de l'article 230-8 du code de procédure pénale, si elles ne le prévoient pas expressément, ne font pas obstacle à ce que le procureur de la République ou le magistrat référent décide d'accueillir une demande d'effacement.

7. Dans les hypothèses mentionnées au point 6, les magistrats compétents pour décider de l'effacement des données prennent en considération la nature et la gravité des faits constatés, les motifs de la relaxe, de l'acquiescement, du non-lieu ou du classement sans suite, le temps écoulé depuis les faits et la durée légale de conservation restant à courir, au regard de la situation personnelle de l'intéressé, protégée par les stipulations de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Ils peuvent prendre ainsi en considération l'âge auquel l'intéressé a commis les faits, son comportement depuis et son attitude vis-à-vis des éventuelles victimes ou son insertion sociale. L'application des dispositions de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales impose également au juge de l'excès de pouvoir d'exercer un entier contrôle sur la décision prise par les autorités désignées par la loi sur les demandes d'effacement des données.

8. Enfin, ces règles en matière d'effacement s'exercent sans préjudice de l'obligation pour l'autorité compétente de faire droit aux demandes fondées de rectification ou de mise à jour. Le présent avis sera notifié au tribunal administratif de Montreuil, à M. B...A...et au garde des sceaux, ministre de la justice. Il sera publié au Journal officiel de la République française.

C. Jurisprudence judiciaire

- Cass. crim. 9 avril 2008, n° 07-85972

LA COUR DE CASSATION, CHAMBRE CRIMINELLE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :

- LE PROCUREUR GÉNÉRAL PRÈS LA COUR D'APPEL DE GRENOBLE,

contre l'arrêt n° 671 de ladite cour d'appel, chambre correctionnelle, en date du 5 juillet 2007, qui a relaxé Georges X... du chef de refus de se soumettre à un prélèvement biologique ;

Vu les mémoires produits en demande et en défense ;

Sur le moyen unique de cassation, pris de la violation des articles 464, 469-1, 706-54, alinéa 1, et 706-56, II, alinéa 1, du code de procédure pénale ;

"en ce que l'arrêt a renvoyé le prévenu des fins de la poursuite pour avoir refusé de se soumettre au prélèvement biologique destiné à l'identification de son empreinte biologique ;

"au motif que la dispense de peine dont il avait précédemment fait l'objet pour vol aggravé ne constituant pas une condamnation, le prélèvement ne pouvait lui être imposé et qu'en le refusant, il n'avait pas commis l'infraction reprochée ;

"alors que, en le déclarant coupable de vol aggravé avant de le dispenser de peine, le tribunal correctionnel de Grenoble avait prononcé à l'encontre du prévenu une condamnation qui justifiait qu'il se soumette au prélèvement biologique destiné à l'identification de son empreinte génétique, au risque de poursuites en cas de refus" ;

Attendu qu'il résulte de l'arrêt attaqué que, le 16 février 2004, le procureur de la République de Grenoble a requis un prélèvement biologique destiné à permettre l'identification de l'empreinte génétique de Georges X... déclaré coupable de vol aggravé par jugement du tribunal correctionnel, en date du 19 septembre 2003, qui l'a

dispensé de peine ; qu'ayant refusé, le 12 octobre 2005, de se soumettre au prélèvement, l'intéressé a été poursuivi sur le fondement de l'article 706-56 du code de procédure pénale ;

Attendu que, pour infirmer le jugement et relaxer le prévenu, l'arrêt retient que la dispense de peine ne constitue pas une condamnation permettant en application des dispositions de l'article 706-54, alinéa 1, du code de procédure pénale l'inscription au fichier national automatisé des empreintes génétiques ;

Attendu qu'en prononçant ainsi, la cour d'appel a fait l'exacte application de la loi ;

D'où il suit que le moyen doit être écarté ;

Et attendu que l'arrêt est régulier en la forme ;

REJETTE le pourvoi ;

II. Constitutionnalité de la disposition contestée

A. Normes de référence

Déclaration des droits de l'homme et du citoyen de 1789

- Article 2

Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression.

B. Jurisprudence du Conseil constitutionnel

Sur l'atteinte au droit au respect de la vie privée

- Décision n° 99-416 DC du 23 juillet 1999 - Loi portant création d'une couverture maladie universelle

. En ce qui concerne l'article 36 :

43. Considérant que l'article 36 modifie les articles L. 161-31 et L. 162-1-6 du code de la sécurité sociale relatifs au contenu et à l'utilisation d'une "carte électronique individuelle inter-régimes" ainsi qu'à sa délivrance à tout bénéficiaire de l'assurance maladie ;

44. Considérant que les requérants font grief à ce dispositif de porter atteinte au respect de la vie privée ; qu'ils font valoir que le système informatisé de transmission d'informations relatives à la santé des titulaires de la carte ne présente pas toutes les garanties et " comporte le risque d'être déjoué " ;

45. Considérant qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : " Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression. " ; que la liberté proclamée par cet article implique le respect de la vie privée ;

46. Considérant qu'aux termes du I de l'article L. 161-31 du code de la sécurité sociale, la carte électronique individuelle " doit permettre d'exprimer de manière précise l'accord du titulaire ou de son représentant légal pour faire apparaître les éléments nécessaires non seulement à la coordination des soins mais aussi à un suivi sanitaire " ; que le II du même article dispose : " Dans l'intérêt de la santé du patient, cette carte comporte un volet de santé... destiné à ne recevoir que les informations nécessaires aux interventions urgentes ainsi que les éléments permettant la continuité et la coordination des soins " ; qu'en vertu du I de l'article L.162-1-6 du code de la sécurité sociale, l'inscription, sur la carte, de ces informations est subordonnée dans tous les cas à l'accord du titulaire ou, s'agissant d'un mineur ou d'un majeur incapable, de son représentant légal ; que les personnes habilitées à donner cet accord peuvent, par ailleurs, " conditionner l'accès à une partie des informations contenues dans le volet de santé à l'utilisation d'un code secret qu'elles auront-elles-mêmes établi " ; que l'intéressé a accès au contenu du volet de santé par l'intermédiaire d'un professionnel de santé habilité ; qu'il dispose du droit de rectification, du droit d'obtenir la suppression de certaines mentions et du droit de s'opposer à ce que, en cas de modification du contenu du volet de santé, certaines informations soient mentionnées ; qu'en outre, il appartiendra à un décret en Conseil d'État, pris après avis public et motivé du Conseil national de l'Ordre des médecins et de la Commission nationale de l'informatique et des libertés, de fixer la nature des informations portées sur le volet de santé, les modalités d'identification des professionnels ayant inscrit des informations sur ce volet, ainsi que les conditions dans lesquelles, en fonction des types d'information, les professionnels de santé seront habilités à consulter, inscrire ou effacer les informations ; que la méconnaissance des règles permettant la communication d'informations figurant sur le volet de santé, ainsi que celle des règles relatives à la modification des informations, seront réprimées dans les conditions prévues par le VI de l'article L. 162-1-6 du code de la sécurité sociale ; que les sanctions pénales prévues par ces dernières dispositions s'appliqueront sans préjudice des dispositions de la section V du chapitre VI du titre II du livre deuxième du code pénal intitulée " Des atteintes aux droits de la personne résultant des fichiers ou des traitements

informatiques " ; qu'enfin, le législateur n'a pas entendu déroger aux dispositions de l'article 21 de la loi du 6 janvier 1978 susvisée relatives aux pouvoirs de surveillance et de contrôle de la Commission nationale de l'informatique et des libertés ;

47. Considérant que l'ensemble des garanties dont est assortie la mise en œuvre des dispositions de l'article 36 de la loi, au nombre desquelles il convient de ranger les caractéristiques assurant la sécurité du système, sont de nature à sauvegarder le respect de la vie privée ;

- **Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure**

- Quant au respect de la vie privée :

21. Considérant que le I de l'article 21 prévoit que : " Les services de la police nationale et de la gendarmerie nationale peuvent mettre en oeuvre des applications automatisées d'informations nominatives recueillies au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'Etat, afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs " ; qu'aux termes du II du même article : " Les traitements mentionnés au I peuvent contenir des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées au premier alinéa du I. - Ils peuvent également contenir des informations sur les victimes de ces infractions ; ces dernières peuvent toutefois s'opposer à ce que les informations nominatives les concernant soient conservées dans le fichier dès lors que l'auteur des faits a été définitivement condamné " ;

22. Considérant que le III de l'article 21 place le traitement des informations nominatives sous le contrôle du procureur de la République compétent ; que celui-ci peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire ; que la rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande ; qu'en cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention ; que les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles ;

23. Considérant que le IV de l'article 21 définit strictement les personnes, autres que les magistrats judiciaires, habilités, en raison de leurs attributions de police judiciaire, à utiliser les traitements en cause ; qu'en vertu du V du même article : " Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article. Il précise notamment la liste des contraventions mentionnées au I, la durée de conservation des informations enregistrées, les modalités d'habilitation des personnes mentionnées au IV ainsi que, le cas échéant, les conditions dans lesquelles les personnes intéressées peuvent exercer leur droit d'accès " ;

24. Considérant que l'article 22 de la loi déferée, qui modifie l'article 39 de la loi du 6 janvier 1978 susvisée, fixe les conditions et modalités selon lesquelles les données nominatives contenues dans les fichiers intéressant en particulier la sécurité publique peuvent être communiquées aux personnes intéressées ;

25. Considérant que l'article 23 dresse limitativement la liste des décisions judiciaires au titre desquelles une personne peut être inscrite dans le fichier des personnes recherchées ;

26. Considérant, enfin, ainsi qu'il ressort des débats parlementaires, que la loi du 6 janvier 1978 susvisée, que le législateur n'a pas entendu écarter, s'appliquera aux traitements en cause ;

27. Considérant que l'ensemble de ces garanties est de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée

- Quant à l'utilisation des traitements à des fins administratives :

28. Considérant que l'article 25 ne permet la consultation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire que pour des finalités déterminées ;

29. Considérant qu'il s'agit, en premier lieu, " des décisions de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y

exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux " ; qu'en pareil cas, la consultation a pour but exclusif de vérifier que le comportement des intéressés n'est pas incompatible avec l'exercice des fonctions ou missions envisagées ; qu'elle s'effectue dans la stricte mesure exigée par la protection de la sécurité des personnes et par la défense des intérêts fondamentaux de la Nation ; qu'elle donne lieu à information des intéressés ; qu'un décret en Conseil d'Etat doit fixer la liste des enquêtes administratives qui, en application de l'article 25 de la loi déferée, pourront donner lieu à la consultation des traitements automatisés d'informations personnelles mentionnés à son article 21 ;

30. Considérant que la consultation est également prévue " pour l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux " ; qu'en pareil cas, la consultation est faite par des agents de la police et de la gendarmerie spécialement habilités à cet effet ou, dans des conditions déterminées par décret en Conseil d'Etat, par des personnels investis de missions de police administrative désignés selon les mêmes procédures ;

31. Considérant que la consultation est enfin permise pour " l'exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, ainsi qu'au titre des mesures de protection ou de défense prises dans les secteurs de sécurité des installations prioritaires de défense visés à l'article 17 de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense " ; qu'en pareil cas, la consultation est effectuée par des agents de la police et de la gendarmerie nationale spécialement habilités à cet effet ;

32. Considérant qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées ;

33. Considérant qu'eu égard aux motifs qu'elle fixe pour ces consultations, comme aux restrictions et précautions dont elle les assortit, la loi déferée ne méconnaît par elle-même aucune des exigences constitutionnelles ci-dessus mentionnées ;

34. Considérant, en outre, qu'en vertu de l'article 2 de la loi du 6 janvier 1978 susvisée, que ne remettent pas en cause les dispositions contestées : " Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé " ; que les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative ;

35. Considérant, enfin, que ces dispositions ne portent pas par elles-mêmes atteinte aux droits des étrangers, lesquels ne comprennent aucun droit de caractère général et absolu d'acquérir la nationalité française ou de voir renouveler leur titre de séjour ; qu'elles ne sauraient en revanche être entendues comme remettant en cause l'acquisition de la nationalité française lorsque celle-ci est, en vertu de la loi, de plein droit, ni le renouvellement d'un titre de séjour lorsque celui-ci est, en vertu de la loi, de plein droit ou lorsqu'il est commandé par le respect du droit de chacun à mener une vie familiale normale ;

- Quant au principe fondamental reconnu par les lois de la République en matière de droit pénal des mineurs :

36. Considérant que l'atténuation de la responsabilité pénale des mineurs en fonction de l'âge, comme la nécessité de rechercher leur relèvement éducatif et moral par des mesures adaptées à leur âge et à leur personnalité, prononcées par une juridiction spécialisée ou selon des procédures appropriées, ont été constamment reconnues par les lois de la République depuis le début du vingtième siècle ; que ces principes trouvent notamment leur expression dans la loi du 12 avril 1906 sur la majorité pénale des mineurs, la loi du 22 juillet 1912 sur les tribunaux pour enfants et l'ordonnance du 2 février 1945 sur l'enfance délinquante ;

37. Considérant que ce principe n'est pas méconnu du seul fait que les dispositions contestées ne comportent pas de limitation quant à l'âge des personnes sur lesquelles sont recueillies des informations dans les conditions prévues à l'article 21 de la loi déferée ;

38. Considérant toutefois qu'il appartiendra au décret prévu au V de l'article 21 de la loi déferée de déterminer une durée de conservation conciliant, d'une part, la nécessité d'identifier les auteurs d'infractions et, d'autre part, celle de rechercher le relèvement éducatif et moral des mineurs délinquants ;

- Quant au respect de la présomption d'innocence :

39. Considérant qu'aux termes de l'article 9 de la Déclaration de 1789 : " Tout homme étant présumé innocent, jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimé par la loi " ;

40. Considérant, en premier lieu, que l'enregistrement de données nominatives dans des traitements de la nature de ceux auxquels fait référence l'article 21 de la loi déferée ne porte par lui-même aucune atteinte au principe de la présomption d'innocence ;

41. Considérant, en deuxième lieu, qu'en cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées ; que, si le procureur de la République peut en prescrire le maintien " pour des raisons liées à la finalité du fichier ", cette exception à la règle générale d'effacement ne peut être justifiée que par des nécessités d'ordre public appréciées par l'autorité judiciaire ; qu'il est alors fait mention de la décision de relaxe ou d'acquiescement dans le fichier ;

42. Considérant, en troisième lieu, qu'en cas de décision de non lieu ou de classement sans suite, les données personnelles concernant les personnes mises en cause sont conservées sauf si le procureur de la République en ordonne l'effacement ; que, s'il ne le fait pas, les décisions de non lieu et, lorsqu'ils sont motivés par une insuffisance de charges, les classements sans suite font l'objet d'une mention dans le fichier ; qu'il appartiendra ainsi à l'autorité judiciaire d'apprécier dans chaque cas, compte tenu des motifs de la décision prise, si les nécessités de l'ordre public justifient ou non le maintien des données en cause ;

43. Considérant, enfin, ainsi qu'il a été dit ci-dessus, que toute personne inscrite dans le fichier devra pouvoir exercer son droit d'accès et de rectification des données la concernant dans les conditions prévues par l'article 39 de la loi du 6 janvier 1978 susvisée ;

- **Décision n° 2010-25 QPC du 16 septembre 2010 - M. Jean-Victor C. (Fichier empreintes génétiques)**

. En ce qui concerne le prélèvement et l'enregistrement des empreintes génétiques :

12. Considérant, en premier lieu, que, si, dans les cas prévus aux deuxième et troisième alinéas de l'article 706-54, un officier de police judiciaire peut décider d'office un prélèvement biologique aux fins de rapprochement ou de conservation au fichier, un tel acte, nécessairement accompli dans le cadre d'une enquête ou d'une instruction judiciaires, est placé sous le contrôle du procureur de la République ou du juge d'instruction lesquels dirigent son activité conformément aux dispositions du code de procédure pénale ; que les empreintes peuvent être retirées du fichier sur instruction du procureur de la République ; qu'enfin, aux termes du premier alinéa de l'article 706-54, le fichier est placé sous le contrôle d'un magistrat ; que, par suite, le grief tiré de la méconnaissance de l'article 66 de la Constitution doit être écarté ;

13. Considérant, en deuxième lieu, que le prélèvement biologique visé aux deuxième et troisième alinéas de l'article 706-54 ne peut être effectué sans l'accord de l'intéressé ; que, selon le quatrième alinéa du paragraphe I de l'article 706-56, lorsqu'il n'est pas possible de procéder à un prélèvement biologique sur une personne, l'identification de son empreinte génétique peut être réalisée à partir de matériel biologique qui se serait naturellement détaché de son corps ; qu'en tout état de cause, le prélèvement n'implique aucune intervention corporelle interne ; qu'il ne comporte aucun procédé douloureux, intrusif ou attentatoire à la dignité des personnes ;

14. Considérant que, selon le premier alinéa de l'article 706-54, le fichier n'est constitué qu'en vue de faciliter l'identification et la recherche des auteurs de certaines infractions ; qu'à cette fin, le cinquième alinéa de cet article prescrit que : « Les empreintes génétiques conservées dans ce fichier ne peuvent être réalisées qu'à partir de segments d'acide désoxyribonucléique non codants, à l'exception du segment correspondant au marqueur du sexe » ; qu'ainsi, la disposition contestée n'autorise pas l'examen des caractéristiques génétiques des personnes ayant fait l'objet de ces prélèvements mais permet seulement leur identification par les empreintes génétiques ;

15. Considérant qu'en conséquence, manquent en fait les griefs tirés de l'atteinte à l'inviolabilité du corps humain, au principe du respect de la dignité de la personne humaine et à la liberté individuelle ;

16. Considérant, en troisième lieu, que le fichier relève du contrôle de la Commission nationale de l'informatique et des libertés en application des dispositions et selon les modalités prévues par la loi du 6 janvier 1978 susvisée ; que, selon les dispositions de l'article 706-54, il est en outre placé sous le contrôle d'un magistrat ; qu'il est constitué en vue de l'identification et de la recherche des auteurs de certaines infractions et ne centralise que les traces et empreintes concernant les mêmes infractions ; que l'inscription au fichier concerne, outre les personnes condamnées pour ces infractions, celles à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles les aient commises ; que, pour ces dernières, les empreintes prélevées dans le cadre d'une enquête ou d'une information judiciaires sont conservées dans le fichier sur décision d'un officier de police judiciaire agissant soit d'office, soit à la demande du procureur de la République ou du juge d'instruction ; qu'une procédure d'effacement est, dans ce cas, prévue par le législateur, lorsque la conservation des empreintes n'apparaît plus nécessaire compte tenu de la finalité du fichier ; que le refus du

procureur de la République de procéder à cet effacement est susceptible de recours devant le juge des libertés et de la détention dont la décision peut être contestée devant le président de la chambre de l'instruction ; qu'enfin, toute personne bénéficie d'un droit d'accès direct auprès du responsable du fichier en application de l'article 39 de la loi du 6 janvier 1978 susvisée ; que, dès lors, ces dispositions sont de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée ; que le grief tiré de ce que la mise en oeuvre du fichier ne serait pas assortie de garanties appropriées doit être écarté ;

17. Considérant, en quatrième lieu, que le prélèvement biologique aux fins de la conservation au fichier, prévu par le deuxième alinéa de l'article 706-54, des empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves et concordants rendant vraisemblable qu'elles aient commis certaines infractions et le prélèvement biologique aux fins de rapprochement d'empreintes, prévu par le troisième alinéa de l'article 706-54, auquel il peut être procédé sur toute personne à l'encontre de laquelle il existe des raisons plausibles de soupçonner qu'elle a commis l'un de ces mêmes crimes ou délits, n'emportent ni déclaration ni présomption de culpabilité ; qu'ils peuvent au contraire établir l'innocence des personnes qui en sont l'objet ; que l'obligation pénalement sanctionnée de se soumettre au prélèvement, qui n'implique pas davantage de reconnaissance de culpabilité, n'est pas contraire à la règle selon laquelle nul n'est tenu de s'accuser ; que, dès lors, ces dispositions ne portent pas atteinte à la présomption d'innocence ;

18. Considérant, en cinquième lieu, que l'enregistrement au fichier des empreintes génétiques de personnes condamnées pour des infractions particulières ainsi que des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une de ces infractions est nécessaire à l'identification et à la recherche des auteurs de ces crimes ou délits ; que le dernier alinéa de l'article 706-54 renvoie au décret le soin de préciser notamment la durée de conservation des informations enregistrées ; que, dès lors, il appartient au pouvoir réglementaire de proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées tout en adaptant ces modalités aux spécificités de la délinquance des mineurs ; que, sous cette réserve, le renvoi au décret n'est pas contraire à l'article 9 de la Déclaration de 1789 ;

- **Décision n° 2011-625 DC du 10 mars 2011 - Loi d'orientation et de programmation pour la performance de la sécurité intérieure**

- SUR L'ARTICLE 11 :

9. Considérant que l'article 11 codifié aux articles 230-6 à 230-11 du code de procédure pénale, en les modifiant, les dispositions de l'article 21 de la loi du 18 mars 2003 susvisée relatives aux fichiers d'antécédents ;

10. Considérant que les requérants soutiennent que, si, dans sa décision du 13 mars 2003 susvisée, le Conseil constitutionnel a déjà déclaré conformes à la Constitution les dispositions codifiées par l'article 11 de la loi déferée, un changement des circonstances, intervenu depuis cette décision, justifie le réexamen de ces dispositions ; qu'ils font valoir, à cet égard, que la Commission nationale de l'informatique et des libertés a, dans son rapport remis au Premier ministre le 20 janvier 2009 sur le contrôle du Système de traitement des infractions constatées, estimé que, dans une proportion importante, les fiches de personnes mises en cause étaient inexactes et que les dispositions relatives au suivi et aux rectifications de ce fichier étaient « manifestement inefficaces », alors que le nombre de personnes enregistrées est considérable ; qu'ils dénoncent également, comme injustifiée et inintelligible, la différence de régime d'effacement des données instituée par l'article 230-8 du code de procédure pénale, entre les données collectées à l'occasion d'une procédure ayant donné lieu à un classement sans suite, selon que la décision de classement est motivée par une insuffisance de charges ou pour un autre motif ;

11. Considérant que, dans sa décision du 13 mars 2003 susvisée, le Conseil constitutionnel a déclaré l'article 21 ainsi que l'article 25 de la loi du 18 mars 2003 pour la sécurité intérieure conformes à la Constitution sous les réserves mentionnées aux considérants 26, 34, 35, 38 et 43 de sa décision ; qu'il a jugé que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux traitements en cause et que toute personne inscrite dans le fichier doit pouvoir exercer son droit d'accès et de rectification des données qui la concernent dans les conditions prévues par l'article 39 de cette loi ; que, lorsque ces données sont consultées dans le cadre d'enquêtes administratives, elles ne peuvent constituer qu'un élément de la décision prise par l'autorité administrative, sous le contrôle du juge ; que l'utilisation de ces données ne saurait permettre de remettre en cause l'acquisition de la nationalité française lorsque, en vertu de la loi, celle-ci est de plein droit ; qu'elle ne saurait pas davantage interdire le renouvellement d'un titre de séjour lorsque, en vertu de la loi, celui-ci est de plein droit ou lorsqu'il est commandé par le respect du droit de chacun à mener une vie familiale normale ; qu'enfin, s'agissant des mineurs, il appartient au décret de déterminer une durée de conservation

conciliant, d'une part, la nécessité d'identifier les auteurs d'infractions et, d'autre part, celle de rechercher le relèvement éducatif et moral des mineurs délinquants ;

12. Considérant que les modifications apportées aux dispositions de l'article 21 de la loi du 18 mars 2003 susvisées à l'occasion de leur introduction aux articles 230-6 à 230-11 du code de procédure pénale renforcent le contrôle de l'autorité judiciaire sur les données enregistrées dans les fichiers d'antécédents ; que l'article 230-8 du code de procédure pénale prévoit que le procureur de la République ou le magistrat chargé de suivre la mise en oeuvre et la mise à jour des traitements se prononce, dans un délai d'un mois, sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification ; que cet article prévoit également que toutes les données relatives à des personnes mises en cause et maintenues dans les fichiers d'antécédents en dépit d'une décision de relaxe, d'acquiescement, de non-lieu ou de classement sans suite, quel qu'en soit le motif, font l'objet d'une mention qui interdit l'accès à ces données dans le cadre d'une enquête administrative ; que la différence de régime de conservation des données, qui résulte de la faculté donnée au procureur de la République d'ordonner l'effacement lorsque le classement sans suite de la procédure est motivé par une insuffisance de charges, est fondée sur l'absence d'intérêt de conserver, dans ce cas, de telles données dans le fichier ;

13. Considérant qu'il résulte de ce qui précède que, sous les mêmes réserves que celles rappelées au considérant 11, les dispositions des articles 230-6 à 230-11 du code de procédure pénale, qui ne sont ni obscures ni ambiguës, sont conformes à la Constitution ;

- **Décision n° 2012-652 DC du 22 mars 2012 - Loi relative à la protection de l'identité**

- SUR LES ARTICLES 5 et 10 :

2. Considérant que l'article 5 de la loi déferée 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 déferée 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 oeuvre 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 déferée 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 atteinte 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 ;

- Décision n° 2014-690 DC du 13 mars 2014 - Loi relative à la consommation

. En ce qui concerne le grief tiré de l'atteinte au droit au respect de la vie privée :

51. Considérant que la liberté proclamée par l'article 2 de la Déclaration 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 oeuvre de manière adéquate et proportionnée à cet objectif ;

52. Considérant que la création d'un traitement de données à caractère personnel destiné à recenser les crédits à la consommation contractés par les personnes physiques pour leurs besoins non professionnels, les incidents de paiement caractérisés liés aux crédits souscrits par ces personnes ainsi que les informations relatives aux situations de surendettement et aux liquidations judiciaires vise à prévenir plus efficacement et plus précocement les situations de surendettement en fournissant aux établissements et organismes financiers des éléments leur permettant d'apprécier, au moment de l'octroi du prêt, la solvabilité des personnes physiques qui sollicitent un crédit ou se portent caution et en conséquence de mieux évaluer le risque ; que, par la création du registre national des crédits aux particuliers, le législateur a poursuivi un motif d'intérêt général de prévention des situations de surendettement ;

53. Considérant que les informations enregistrées dans le registre national des crédits aux particuliers sont énumérées par le paragraphe IV de l'article L. 333-10 du code de la consommation ; qu'y figureront des informations relatives à l'état civil de la personne qui a souscrit le crédit, à l'identification de l'établissement ou de l'organisme à l'origine de la déclaration, à l'identification, à la catégorie et aux caractéristiques du crédit, aux incidents de paiement caractérisés, aux situations de surendettement et aux liquidations judiciaires prononcées, à la date de mise à jour des données et au motif et à la date des consultations effectuées ; qu'en vertu des dispositions de l'article L. 333-11, les informations relatives aux crédits seront conservées pendant la durée d'exécution du contrat de crédit ; que celles relatives aux incidents de paiement seront conservées jusqu'au

paiement intégral des sommes dues, sans que la durée de conservation de ces informations puisse excéder cinq ans à compter de la date d'enregistrement de l'incident de paiement ; que celles relatives aux situations de surendettement seront conservées pendant la durée de l'exécution du plan ou des mesures, sans que la durée de conservation des informations puisse excéder sept ans ; que celles relatives à la procédure de rétablissement personnel, à la procédure de liquidation judiciaire ou à un effacement partiel de dettes seront conservées jusqu'à l'expiration d'une période de cinq ans à compter de la date d'homologation ou de clôture de la procédure ; que le traitement de données à caractère personnel qui est créé est ainsi destiné à recueillir et à conserver pendant plusieurs années des données précises et détaillées relatives à un grand nombre de personnes physiques débitrices ;

54. Considérant que les dispositions de l'article L. 333-8 du code de la consommation prévoient une consultation obligatoire de ce registre par les établissements et organismes financiers « avant toute décision effective d'octroyer un crédit à la consommation » ainsi qu'« avant de proposer à l'emprunteur de reconduire un contrat de crédit renouvelable et dans le cadre de la vérification triennale de solvabilité de l'emprunteur » ; qu'elles autorisent une consultation de ce registre par les caisses de crédit municipal avant toute décision effective d'octroi d'un prêt sur gage corporel ainsi que par les établissements ou organismes financiers pour les personnes qui se portent caution à l'occasion de l'octroi d'un crédit à la consommation ; qu'elles autorisent également une consultation des seules informations de ce registre relatives aux incidents de paiement caractérisés, aux situations de surendettement et aux liquidations judiciaires par les établissements et organismes financiers « avant qu'ils ne formulent une offre » de prêt immobilier ou de prêt viager hypothécaire et qu'elles prévoient que ces informations peuvent également « être prises en compte par ces mêmes établissements et organismes dans leurs décisions d'attribution des moyens de paiement, ainsi que pour la gestion des risques liés aux crédits souscrits par leurs clients » ; qu'elles interdisent enfin que les informations contenues dans le registre puissent être consultées ou utilisées à d'autres fins que celles expressément prévues, sous peine des sanctions de l'article 226-21 du code pénal ; que la consultation du registre est par ailleurs ouverte, en vertu de l'article L. 333-9, aux commissions de surendettement dans l'exercice de leur mission de traitement des situations de surendettement ainsi qu'aux greffes des tribunaux compétents dans le cadre de la procédure de traitement des situations de surendettement ; que le registre peut ainsi être consulté à de très nombreuses reprises et dans des circonstances très diverses ;

55. Considérant que l'article L. 333-19 autorise les établissements et organismes financiers à utiliser les informations collectées lors de la consultation du registre dans des systèmes de traitement automatisé de données ;

56. Considérant que l'article L. 333-20 subordonne à une autorisation individuelle et une habilitation, selon des procédures spécifiques internes aux établissements et organismes financiers, la consultation du registre par les personnels des établissements et organismes financiers ; qu'en renvoyant à un décret en Conseil d'État les modalités d'application de cette autorisation, le législateur n'a pas limité le nombre de personnes employées par ces établissements et organismes susceptibles d'être autorisées à consulter le registre ;

57. Considérant qu'il résulte de ce qui précède qu'en égard à la nature des données enregistrées, à l'ampleur du traitement, à la fréquence de son utilisation, au grand nombre de personnes susceptibles d'y avoir accès et à l'insuffisance des garanties relatives à l'accès au registre, les dispositions contestées 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 dispositions de l'article 67 doivent être déclarées contraires à la Constitution ; qu'il en va de même, par voie de conséquence, des dispositions des articles 68 à 72, qui en sont inséparables ;

- **Décision n° 2015-727 DC du 21 janvier 2016 - Loi de modernisation de notre système de santé**

- SUR CERTAINES DISPOSITIONS DE L'ARTICLE 178 :

87. Considérant que le 5° de l'article 178 modifie l'article L. 1453-1 du code de la santé publique pour renforcer la transparence des liens d'intérêt entre, d'une part, les entreprises produisant ou commercialisant des produits à finalité sanitaire ou cosmétique destinés à l'homme mentionnés au paragraphe II de l'article L. 5311-1 ou les entreprises assurant des prestations associées à ces produits et, d'autre part, les acteurs du secteur de la santé énumérés au paragraphe I de l'article L. 1453-1 ; que le a) du 5° de l'article 178 modifie le paragraphe I de l'article L. 1453-1 pour prévoir que les entreprises sont tenues de rendre publics, sur un site internet public unique, l'objet précis, la date, le bénéficiaire direct, le bénéficiaire final et le montant des conventions conclues avec les acteurs du secteur de la santé ; que, toutefois, pour les produits cosmétiques, les produits de tatouage et les lentilles oculaires non correctrices, les entreprises sont seulement tenues de rendre publique l'existence de conventions ; que, pour tous les types de produits à finalité sanitaire ou cosmétique, les conventions ayant pour

objet l'achat de biens ou services sont exclues du champ de ces obligations de publicité ; que le b) du 5° insère, dans l'article L. 1453-1, un nouveau paragraphe I bis, qui prévoit que sont rendues publiques, lorsqu'elles excèdent un seuil fixé par décret, les rémunérations versées aux acteurs du secteur de la santé ; qu'en vertu du paragraphe II de l'article L. 1453-1 doivent également être rendus publics les avantages en nature ou en espèces, autres que les rémunérations, versés aux acteurs du secteur de la santé ; que le d) du 5° de l'article 178 insère, dans l'article L. 1453-1, un nouveau paragraphe II bis qui prévoit que les informations ainsi rendues publiques sont réutilisables à titre gratuit et peuvent donner lieu à un traitement de données ;

88. Considérant que les députés requérants font grief aux obligations de publicité prévues par le 5° de l'article 178 de méconnaître le principe de légalité des délits et des peines et l'objectif d'accessibilité et d'intelligibilité de la loi en ne définissant pas précisément la nature des informations devant être rendues publiques ; qu'ils reprochent également à l'obligation de publicité prévue au premier alinéa du paragraphe I de l'article L. 1453-1 de porter atteinte à la liberté d'entreprendre ; qu'ils soutiennent, enfin, que les obligations de publicité prévues par les paragraphes I, I bis et II de l'article L. 1453-1 méconnaissent le droit au respect de la vie privée, garanti par l'article 2 de la Déclaration de 1789 ;

89. Considérant, en premier lieu, que les dispositions du 5° de l'article 178 ne créent aucune incrimination ; que, par suite, le grief tiré de la méconnaissance du principe de légalité des délits et des peines doit être écarté ;

90. Considérant, en deuxième lieu, que l'obligation, prévue au premier alinéa du paragraphe I de l'article L. 1453-1, de rendre publics l'objet précis, la date, le bénéficiaire direct, le bénéficiaire final et le montant des conventions est justifiée par l'exigence constitutionnelle de protection de la santé et par l'objectif d'intérêt général de prévention des conflits d'intérêt ; que cette obligation exclut de son champ d'application les conventions ayant pour objet l'achat de biens ou services ; qu'ainsi en mettant une telle obligation à la charge des entreprises produisant ou commercialisant des produits à finalité sanitaire destinés à l'homme et des produits à finalité cosmétique et des entreprises assurant des prestations associées à ces produits, le législateur n'a pas porté une atteinte manifestement disproportionnée à la liberté d'entreprendre ; que, par suite, le grief tiré de la méconnaissance de la liberté d'entreprendre doit être écarté ;

91. Considérant, en troisième lieu, qu'aux termes de l'article 2 de la Déclaration de 1789 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression » ; que la liberté proclamée par cet article implique le droit au respect de la vie privée ; que la publicité d'informations relatives à des conventions passées entre des personnes privées, physiques ou morales, contenant des données à caractère personnel relevant de la vie privée porte atteinte au respect de la vie privée ; que, pour être conformes à la Constitution, ces atteintes doivent être justifiées par un motif d'intérêt général et mises en œuvre de manière adéquate et proportionnée à cet objectif ;

92. Considérant que l'obligation de rendre publics, sur un site internet public unique, l'objet précis, la date, l'identité du bénéficiaire direct, l'identité du bénéficiaire final, le montant, y compris les rémunérations et les avantages en nature ou en espèces, des conventions conclues par les entreprises produisant ou commercialisant des produits à finalité sanitaire destinés à l'homme ou assurant des prestations associées à ces produits avec les autres acteurs du secteur de la santé porte atteinte au droit au respect de la vie privée ; que cette publication est destinée à garantir l'exhaustivité des informations relatives à l'existence et à la nature des liens d'intérêt entre les professionnels de santé et ces entreprises ; que cette atteinte est justifiée par l'exigence constitutionnelle de protection de la santé et par l'objectif d'intérêt général de prévention des conflits d'intérêt ; que, eu égard aux exigences particulières qui pèsent sur les acteurs du secteur de la santé et à la gravité des conséquences des conflits d'intérêt dans ce secteur, le législateur a opéré une conciliation qui n'est pas manifestement déséquilibrée entre les principes constitutionnels en cause ; que, par suite, le grief tiré de la méconnaissance du droit au respect de la vie privée doit être écarté ;

93. Considérant qu'il résulte de ce qui précède que les dispositions du 5° de l'article 178, qui ne méconnaissent aucune autre exigence constitutionnelle, doivent être déclarées conformes à la Constitution ;

- **Décision n° 2016-591 QPC du 21 octobre 2016 - Mme Helen S. (Registre public des trusts)**

Sur le fond :

3. 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. 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.

4. Le registre public des trusts institué par le deuxième alinéa de l'article 1649 AB du code général des impôts recense tous les trusts, au sens de l'article 792-0 bis du même code, dont la déclaration est rendue obligatoire par

les premier et cinquième alinéas du même article. Ces trusts sont ceux dont l'administrateur, le constituant ou au moins l'un des bénéficiaires a son domicile fiscal en France ou ceux qui comprennent un bien ou un droit qui y est situé. Pour chaque trust recensé, ce registre précise la date de sa constitution ainsi que les noms de son administrateur, de son constituant, et de ses bénéficiaires. Le quatrième alinéa de l'article 1649 AB renvoie à un décret en Conseil d'État le soin de préciser les modalités de consultation de ce registre public.

5. En favorisant, par les dispositions contestées, la transparence sur les trusts, le législateur a entendu éviter leur utilisation à des fins d'évasion fiscale et de blanchiment des capitaux. Il a ainsi poursuivi l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales.

6. La mention, dans un registre accessible au public, des noms du constituant, des bénéficiaires et de l'administrateur d'un trust fournit des informations sur la manière dont une personne entend disposer de son patrimoine. Il en résulte une atteinte au droit au respect de la vie privée. Or, le législateur, qui n'a pas précisé la qualité ni les motifs justifiant la consultation du registre, n'a pas limité le cercle des personnes ayant accès aux données de ce registre, placé sous la responsabilité de l'administration fiscale. Dès lors, les dispositions contestées portent au droit au respect de la vie privée une atteinte manifestement disproportionnée au regard de l'objectif poursuivi. Par conséquent, sans qu'il soit besoin d'examiner les autres griefs, le deuxième alinéa de l'article 1649 AB du code général des impôts doit être déclaré contraire à la Constitution.

- **Décision n° 2016-744 DC du 29 décembre 2016 - Loi de finances pour 2017**

. En ce qui concerne le grief tiré de l'atteinte au droit au respect de la vie privée :

61. Aux termes de l'article 2 de la Déclaration de 1789 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression ». La liberté proclamée par cet article implique le droit au respect de la vie privée. 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.

62. Le premier alinéa du 1 de l'article 1671 du code général des impôts, rétabli par le 17° du B du paragraphe I de l'article 60, confie le prélèvement à la source sur les revenus salariaux et de remplacement au débiteur de ces revenus. À cette fin, la première phrase du premier alinéa du 2 de l'article 1671 du code général des impôts prévoit que ce dernier applique le taux calculé et transmis par l'administration.

63. En prévoyant, en principe, la communication par l'administration au débiteur des revenus salariaux et de remplacement d'un taux applicable au prélèvement, le législateur a porté une atteinte au droit au respect de la vie privée du contribuable. Toutefois, d'une part, cette atteinte est justifiée par l'intérêt général qui s'attache à la mise en place du prélèvement à la source pour éviter que les contribuables subissent un décalage d'un an entre la perception des revenus et le paiement de l'impôt. D'autre part, le contribuable titulaire de revenus salariaux ou de remplacement peut, en vertu de l'article 204 H du code général des impôts, opter pour le taux par défaut, lequel ne révèle pas le taux d'imposition de son foyer. Par conséquent, la première phrase du premier alinéa du 2 de l'article 1671 du code général des impôts ne méconnaît pas le droit au respect de la vie privée.

- **Décision n° 2016-745 DC du 26 janvier 2017 - Loi relative à l'égalité et à la citoyenneté**

- Sur certaines dispositions de l'article 78 :

22. L'article L. 411-10 du code de la construction et de l'habitation prévoit que le ministère chargé du logement tient un répertoire des logements locatifs sociaux et de leurs habitants, pour permettre l'élaboration et la mise en œuvre des politiques publiques de l'habitat.

23. Le c du 1° du paragraphe I de l'article 78 de la loi déferée complète cet article L. 411-10. Il prévoit que, pour alimenter ce répertoire, les bailleurs sociaux transmettent au ministère chargé du logement le numéro d'immatriculation au répertoire national d'identification des personnes physiques de chaque occupant majeur d'un logement locatif social.

24. Les sénateurs requérants soutiennent que ces dispositions portent une atteinte injustifiée au droit au respect de la vie privée des occupants de logements sociaux.

25. 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. 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.

26. En adoptant les dispositions contestées, le législateur a entendu que le ministère chargé du logement soit en mesure d'établir une cartographie de l'occupation socio-économique du parc de logements sociaux, afin d'améliorer la mise en œuvre de la politique en matière d'attribution de ces logements. Il a ainsi poursuivi un objectif d'intérêt général.

27. Si les collectivités territoriales et certains de leurs établissements publics peuvent obtenir du représentant de l'État dans la région les informations relatives aux logements situés sur leur territoire contenues dans le répertoire, c'est en vertu du huitième alinéa de l'article L. 411-10, à la condition que ces informations aient été préalablement rendues anonymes.

28. Par ailleurs, le législateur a prévu au 4° du paragraphe I de l'article 78 que l'exploitation des données du répertoire par le groupement d'intérêt public mentionné à l'article L. 441-2-1 du code de la construction et de l'habitation est réalisée de manière à rendre impossible l'identification des intéressés.

29. Il en résulte que le législateur a retenu des modalités de collecte, d'enregistrement, de conservation, et de communication du numéro d'immatriculation au répertoire national d'identification des personnes physiques adéquates et proportionnées à l'objectif poursuivi. Par conséquent, le grief tiré de la méconnaissance du droit au respect de la vie privée doit être écarté.

30. Le c du 1° du paragraphe I de l'article 78 de la loi déferée, qui ne méconnaît aucune autre exigence constitutionnelle, est conforme à la Constitution.

- **Décision n° 2017-637 QPC du 16 juin 2017 - Association nationale des supporters (Refus d'accès à une enceinte sportive et fichier d'exclusion)**

- Sur le troisième alinéa de l'article L. 332-1 du code du sport :

10. La liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. 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.

11. Le troisième alinéa de l'article L. 332-1 du code du sport permet aux organisateurs de manifestations sportives à but lucratif d'établir un traitement automatisé de données à caractère personnel recensant les personnes qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité de ces manifestations.

12. En autorisant l'établissement d'un tel fichier, le législateur a entendu renforcer la sécurité des manifestations sportives à but lucratif, en permettant à leurs organisateurs d'identifier les personnes susceptibles d'en compromettre la sécurité. Il a ainsi poursuivi un objectif d'intérêt général.

13. Il ressort du texte adopté et des débats parlementaires que, par ces dispositions, le législateur n'a pas entendu déroger aux garanties apportées par la loi du 6 janvier 1978 mentionnée ci-dessus relatives notamment aux pouvoirs de la Commission nationale de l'informatique et des libertés, qui s'appliquent aux traitements en cause.

14. Le fichier prévu par les dispositions contestées ne peut être établi que par les organisateurs de manifestations sportives à but lucratif. Il ne peut recenser que les personnes qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité de ces manifestations. Il ne peut être employé à d'autres fins que l'identification desdites personnes en vue de leur refuser l'accès à des manifestations sportives à but lucratif. Il en résulte que le traitement de données prévu par les dispositions contestées est mis en œuvre de manière adéquate et proportionnée à l'objectif d'intérêt général poursuivi.

15. Par suite, les dispositions du troisième alinéa de l'article L. 332-1 du code du sport, qui ne méconnaissent ni le droit au respect de la vie privée, ni aucun autre droit ou liberté que la Constitution garantit, doivent être déclarées conformes à la Constitution.