ZRIBI & TEXIER
Avocats au Conseil d'Etat et à la Cour de cassation
01 45 51 51 61
avocats-conseils@zribi-texier.fr
http://www.zribi-texier.fr

CONSEIL D'ETAT

SECTION DU CONTENTIEUX

MEMOIRE COMPLEMENTAIRE

POUR : Le Collectif d'Action Contre l'Enfouissement des Déchets Radioactifs et autres

CONTRE : Le décret n° 2024-323 du 8 avril 2024 portant autorisation d'un traitement automatisé de données à caractère personnel relatif à la sécurité des établissements, ouvrages, installations et activités nucléaires dénommé « *traitement d'optimisation des données et informations d'intérêt nucléaire* »

Sur le recours n° n° 494945

FAITS ET PROCEDURE

I. Le décret n° 2024-323 du 8 avril 2024 porte autorisation d'un traitement automatisé de données à caractère personnel relatif à la sécurité des établissements, ouvrages, installations et activités nucléaires dénommé « traitement d'optimisation des données et informations d'intérêt nucléaire ».

La notice indique que ce décret autorise la création d'un traitement automatisé de données à caractère personnel « *permettant la collecte et l'exploitation des informations permettant de prévenir les atteintes à la sécurité nucléaire, de contrôler et suivre les demandes d'accès aux établissements, ouvrages, installations impliquant des matières nucléaires ou des sources de rayonnements ionisants et les demandes d'autorisation en lien avec les activités nucléaires ainsi que de traiter et suivre les demandes d'habilitation au secret de la défense nationale intéressant le domaine de la filière nucléaire* ».

En particulier, le traitement vise le commandement spécialisé pour la sécurité nucléaire, la gendarmerie nationale et la police nationale, les personnes impliquées dans un évènement susceptible de porter atteinte à la sécurité nucléaire, les personnes faisant l'objet ou ayant fait l'objet d'une demande d'autorisation ou d'habilitation.

De très nombreuses données personnelles sont enregistrées dans le fichier à savoir de nombreux éléments d'identification des personnes physiques dont l'enregistrement tient à leur « *implication* » dans un « *événement susceptible de porter atteinte à la sécurité nucléaire* ».

C'est notamment l'identité, les coordonnées, la situation tant professionnelle que familiale de ces personnes qui sont enregistrées, voire *la prétendue origine raciale ou l'origine ethnique, les opinions politiques*

Et l'enregistrement automatisé des données de ces personnes physiques tient à leur implication dans des « *événements révélant un risque d'atteinte à la sécurité nucléaire* », sans qu'aucune précision ne soit apportée sur la nature de tels événements.

II. Une requête en excès de pouvoir a été déposée le 6 juin dernier devant le Conseil d'Etat (n° 494945) par les exposants, aux fins d'annulation dudit décret.

Parmi les requérants se trouvent plusieurs associations intervenant dans le domaine du nucléaire et certains de leurs membres, lesquels participent à divers événements destinés à sensibiliser le public sur les dangers de cette énergie ; mais pas seulement.

On y trouve également des avocats, par exemple, qui interviennent régulièrement dans des procédures, notamment administratives, touchant à l'activité nucléaire.

On y trouve encore des membres de l'Assemblée nationale ( ) dont les prises de position en matière nucléaire sont publiques.

On y trouve aussi un journaliste auteur de nombreux articles critiques sur la politique du nucléaire en France.

DISCUSSION

III. Le décret attaqué autorise la création d'un traitement automatisé de données à caractère personnel de personnes physiques impliquées dans un événement « *susceptible de porter atteinte* » à la sécurité nucléaire et de personnes faisant l'objet ou ayant fait l'objet d'une demande d'autorisation ou d'habilitation.

Les informations personnelles susceptibles d'être traitées sont très nombreuses et sensibles : « *1° Motif de l'enregistrement ; 2° Éléments d'identification : a) Nom de naissance ; b) Nom d'usage ; c) Prénoms ; d) Surnom, alias ; e) Sexe ; f) Date et lieu de naissance (département/pays) ; g) Nationalité ; h) Signes physiques particuliers et objectifs ; i) Photographies ; j) Documents d'identité (type, numéro, autorité, date et lieu de délivrance) ; k) Origine géographique (lieux de résidence et zone d'activité) ; 3° Coordonnées : a) Numéros de téléphone ; b) Adresses postales et électroniques ; c) Identifiants utilisés (pseudonymes, sites ou réseaux concernés, autres identifiants techniques), à l'exclusion des mots de passe ; 4° Situation : a) Situation familiale ; b) Formation et compétences ; c) Profession et emplois occupés ; d) Moyens de déplacements (moyens utilisés, immatriculation des véhicules, permis de conduire) ; e) Situation au regard de la réglementation de l'entrée et du séjour en France ; 5° Évènements révélant un risque d'atteinte à la sécurité nucléaire : a) Catégorie d'évènement ; b) Nature, date, heure, lieu et description des faits caractérisant le risque d'atteinte ; c) Photographies de l'événement ; 6° Facteurs de dangerosité : a) Lien avec des groupes extrémistes ; b) Éléments ou signes de radicalisation ; c) Données relatives aux troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur ; d) Détention d'armes ; e) Détention d'animaux dangereux ; f) Formation ou technicité au maniement d'armes ou d'explosifs ; g) Autorisation ou refus d'autorisation, habilitation ou refus d'habilitation ou abrogation de l'habilitation à connaître des informations ou supports classifiés : zones, activités ou niveau d'habilitation concernés ; date d'obtention ou de refus de l'autorisation ou de l'habilitation ou date de l'abrogation de l'habilitation ; date de transmission et sens de l'avis et de la décision d'autorisation ou d'habilitation ; emploi, mission ou fonction au titre desquels l'avis est demandé ; 7° Indication de l'enregistrement ou non de la personne dans les traitements de données à caractère personnel suivants : a) Le traitement automatisé de données à caractère personnel dénommé Prévention des atteintes à la sécurité publique mentionné aux articles R. 236-11 et suivants du code de la sécurité intérieure ; b) Le traitement automatisé de données à caractère personnel dénommé Gestion de l'information et prévention des atteintes à la sécurité publique mentionné aux articles R. 236-21 et suivants du code de la sécurité intérieure ; c) Le fichier des personnes*

recherchées prévu par le décret n° 2010-569 du 28 mai 2010 portant création du fichier des personnes recherchées ; d) Le fichier des objets et des véhicules signalés prévu par l'arrêté du 7 juillet 2017 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé : « Fichier des objets et des véhicules signalés » ; e) L'application informatique du système d'information européen concernant les véhicules et les permis de conduire (EUCARIS) ; f) Le traitement automatisé de données à caractère personnel dénommé FSPRT mentionné au 12 de l'article 1er du décret n° 2007-914 du 15 mai 2007 modifié pris pour application du I de l'article 33 de la loi n° 78-17 du 6 janvier 1978 susvisée relative à l'informatique, aux fichiers et aux libertés » (article 2).

Et aux termes de l'article 5 du décret, « *Le traitement peut collecter des données à caractère personnel de la nature de celles mentionnées au I de l'article 6 de la loi du 6 janvier 1978 susvisée, à l'exception des données génétiques et biométriques ainsi que des données concernant la vie sexuelle ou l'orientation sexuelle, dans la stricte mesure où ces données sont nécessaires à la poursuite des finalités définies à l'article 1er* »

Peuvent donc également être collectées les « *données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique* », dont le traitement est en principe interdit (article 6 de la Loi n° 78-17 du 6 janvier 1978).

La création de ce nouveau fichier interroge, alors même qu'en l'absence de réalisation du risque d'atteinte à la sécurité nucléaire, aucun impératif ne justifie la mise en œuvre d'un tel traitement automatisé de données, il existe déjà un traitement automatisé de données à caractère personnel dénommé « *Prévention des atteintes à la sécurité publique* » (article R. 236-11 et suivants du code de la sécurité intérieure) ainsi qu'un traitement automatisé de données à caractère personnel dénommé « *Gestion de l'information et prévention des atteintes à la sécurité publique* » (article R. 236-21 et suivants du code de la sécurité intérieure).

Ce décret ne pourra qu'être censuré.

IV. Aux termes de l'article 4 de la loi du 6 janvier 1978 n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés : « *Les données à caractère personnel doivent être : 1° Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ; 2° Collectées pour des finalités déterminées, explicites et légitimes,*

et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, applicables à de tels traitements et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ; 3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ; 4° Exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ; 5° Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Toutefois, les données à caractère personnel peuvent être conservées au-delà de cette durée dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine ; 6° Traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées ».

Et selon de l'article 6 de la même loi : « *I.- Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. II.- Les exceptions à l'interdiction mentionnée au I sont fixées dans les conditions prévues par le 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 et par la présente loi. III.- De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés suivant les modalités prévues au II de l'article 31 et à l'article 32* ».

Or, on le rappelle, le décret attaqué prévoit la possibilité de traiter certaines de ces données.

Et aux termes de l'article 88 de la même loi, applicable aux traitements relevant de la directive 2016/680 du 27 avril 2016 : « *Le traitement de données mentionnées au I de l'article 6 est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* ».

V. Par ailleurs, aux termes de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDH) : « *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* ».

Si le texte de la Convention ne fait pas référence à des règles de protection spécifiquement applicables en matière de fichiers, la Cour européenne des droits de l'homme porte une attention croissante aux règles de protection applicables dans le domaine, se fondant essentiellement sur l'article 8 de la Convention et sur la Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Dans l'arrêt *MS contre Suède*, la Cour fait ainsi expressément référence à « *la protection des données personnelles [...] qui revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention* » (CEDH, 27 août 1997, n° 20837/92, *MS c/ Suède*).

A cet égard, elle précise que « *même des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics* », d'autant plus lorsque ces données concernent le passé lointain d'une personne (CEDH, 4 mai 2000, *Rotaru c/ Roumanie*, n° 28341/95 ; CEDH, 16 février 2000, *Amann c. Suisse*, n° 27798/95 ; CEDH, 31 mai 2005, *Antunes Rocha c/ Portugal*, n° 64330/01 ; CEDH, 27 octobre 2009, *Haralambie c/ Roumanie*, n° 21737/03 ; CEDH, 17 février 2011, *Wasmuth c/ Allemagne*, n° 12884/03).

Ainsi, c'est en se référant à la Convention 108 du Conseil de l'Europe que la Cour entend la notion de « *données personnelles* » relevant de la « *vie privée* » au sens de l'article 8.

D'une part, elle retient une « *interprétation extensive* » de la vie privée, telle qu'« *aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de "vie privée"* » (CEDH, 16 décembre 1992, *Niemietz c/ Allemagne*, n°13710/88). Cette conception extensive de la vie privée, « *non susceptible d'une définition exhaustive* », recouvre l'intégrité physique et morale de la personne (CEDH, 29 avril 2002, *Pretty c/ Royaume-Uni*, n° 2346/02 ; CEDH, 22 juillet 2003, *Y.F. c/ Turquie*, n° 24209/94).

D'autre part, la Cour entend par données à caractère personnel « *toute information concernant une personne identifiée ou identifiable* » (CEDH, 16 février 2000, *Amman c/ Suisse*).

Ainsi, de nombreux éléments d'identification des personnes entrent-ils dans ce cadre, à commencer par les nom et prénom (CEDH, 22 février 1994, *Burghartz c/ Suisse*, n° 16213/ 0 ; CEDH, 24 octobre 1996, *Guillot c/ France,* n° 22500/93), les données relatives à la santé (CEDH, 27 août 1997*, M. S. c/ Suède,* n° 20837/92), l'identité, l'orientation et la vie sexuelles (CEDH, 6 février 2001, *Bensaïd c/ Royaume-Uni,* n° 44599/98), les origines des personnes (CEDH, 7 février 2002, *Mikulic c/ Croatie,* n° 53176/99 ; CEDH, 13 février 2003, *Odièvre c/ France*, n° 42326/98), ou encore la profession (CEDH, 18 octobre 2011, *Khelili c. Suisse*, n° 16188/07).

En outre, le champ de protection de l'article 8 a bénéficié d'une double extension en matière de mémorisation et d'utilisation des données à caractère personnel.

D'abord, l'arrêt *Rotaru c/ Roumanie* précité (CEDH, 5 mai 2000, n° 28341/95) admet que des données de nature publique – des informations relatives à l'activité politique du requérant, puissent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics.

Ensuite, confrontée à la question des systèmes de vidéosurveillance des lieux publics, la Cour a élargi le champ de la notion de « vie privée » par son arrêt *Peck c/ Royaume-Uni* (CEDH, 28 janvier 2003, n° 44647/98).

S'agissant en particulier des fichiers contenant des données relatives à la vie privée d'un individu autrement dit des données personnelles, la Cour juge que lorsqu'elles sont mémorisées par une autorité publique, leur utilisation et le refus d'accorder la faculté de les réfuter, constituent une ingérence dans le droit au respect de sa vie privée garanti par l'article 8 § 1 de la CESDH.

Aussi, la Cour a apporté une limite à la marge d'appréciation reconnue aux États (CEDH, 26 mars 1987, n° 9248/81, *Leander c/ Suède*), au nom du respect de la démocratie : « *Si la Cour reconnaît que dans une société démocratique, l'existence de services de renseignements peut s'avérer légitime, elle rappelle que le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* » (CEDH, grande ch., 4 mai 2000, n° 28341/95, *Rotaru c/ Roumanie*).

Ainsi, la Cour a jugé que la mémorisation et la communication de données à caractère personnel constituent en tant que telles une ingérence dans le droit au respect de la vie privée s'agissant d'un fichier secret de la police utilisé en cas de candidature d'une personne à un emploi important pour la sécurité nationale, et de l'inscription au fichier national automatisé d'auteurs d'infractions sexuelles (CEDH, 26 mars 1987, n° 9248/81, *Leander c/ Suède* ; CEDH, 17 décembre 2009, n° 5335/06, *Bouchacourt c/ France*).

La Cour européenne exerce un contrôle particulièrement vigilant sur de telles ingérences afin de prévenir les abus d'un système de surveillance secrète des citoyens qui « *comporte le risque de saper, voire de détruire la démocratie au motif de la défendre* » (CEDH, 6 septembre 1978, *Klass c/ Allemagne*, n° 5029/71 ; CEDH, 5 mai 2000, *Rotaru c/ Roumanie,* n° 28341/95).

En effet, le juge européen souligne que la protection des données personnelles est d'une « *importance fondamentale* » pour la jouissance du droit au respect de la vie privée et considère que la divulgation de telles données sans le consentement de l'intéressé doit être justifiée par la défense d'un « *aspect primordial de l'intérêt public* » et s'accompagner de garanties adéquates et suffisantes, notamment un contrôle judiciaire, contre les abus (CEDH, 5 mai 2000, *Rotaru c/ Roumanie,* n° 28341/95 ; CEDH, 25 février 1997, *Z. c/ Finlande,* n° 22009/93).

Aussi, les conséquences de la consultation des fichiers peuvent porter atteinte au droit à la vie privée.

A cet égard, l'inscription dans le fichier Schengen aux fins de non-admission a ainsi été perçue comme une ingérence dans le droit au respect de la vie privée et familiale dès lors que le requérant n'a pu voyager dans les États concernés à titre privé comme à titre professionnel (CEDH, 2 février 2010, *Dalea c/ France*, n° 964/07).

La constitution d'un fichier ayant pour conséquence des interdictions professionnelles automatiques peut tout autant constituer une violation de l'article 8, dès lors qu'une interdiction générale d'occuper un emploi porte en tant que telle atteinte à la « *vie privée* » (CEDH, 27 juillet 2004, *Sidabras et Dziautas c/ Lituanie*, n°s 55480/00 et 59330/00 ; CEDH, 14 février 2006, *Turek c/ Slovaquie*, n° 57986/00).

VI. Dans ce cadre, la Cour opère un contrôle de la légalité de l'ingérence dans la vie privée : « *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* » (CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, n°s 30562/04 et 30566/04, § 103 ; CEDH 18 septembre 2014, *Brunet c/ France*, n° 21010/10, § 35).

A ce titre, la Cour exige de la législation interne qu'elle ménage « *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 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* » (arrêt *S et Marper c. R.U.,* précité.).

Pour s'en assurer, la Cour vérifie le respect du 2nd paragraphe de l'article 8, selon lequel il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit à la vie privée « *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* » (idem).

La Cour examine plusieurs critères parmi lesquels la légalité de l'ingérence, l'existence de garanties suffisantes en matière de droit d'accès et la nécessité de l'ingérence.

Aux termes de l'article 8, § 2, l'ingérence dans le droit au respect à la vie privée doit en effet être prévue par la loi, c'est-à-dire qu'elle doit avoir une base en droit interne, sachant que la Cour entend largement la notion de « loi », en y incluant les textes de rang infra-législatif et le droit non écrit (CEDH, 24 avril 1990, *Krüslin c/ France*, n° 11801/85).

Afin d'éviter toute forme d'arbitraire, cette base interne doit être compatible avec la prééminence du droit et donc « *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. […] elle doit […] définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes* » (CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, § 95 ; CEDH, 4 mai 2000, *Rotaru c/ Roumanie*, n° 28341/95, § 55).

A cet égard, elle a considéré que le fait de conserver des données dans un fichier créé par un arrêté qui n'a fait l'objet d'aucune publication et n'a pas été rendu accessible au public constitue une violation du droit au respect à la vie privée (CEDH, 21 juin 2011, *Shimovolos c/ Russie*, n° 30194/09).

Il en va de même en cas de mémorisation dans un fichier de police de l'identité, des empreintes digitales et de photographies de délinquants sur la base d'une simple instruction non publique, confidentielle et réservée à l'usage interne du ministère des Affaires intérieures, dès lors que le requérant n'a pas pu en prendre connaissance pour en prévoir les conséquences (CEDH, 10 février 2011, *Dimitrov-Kazakov c/ Bulgarie*, n° 11379/03, § 33).

Même dans l'hypothèse d'une base textuelle accessible, la Cour considère que le niveau de précision requis de la législation interne « *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* » (CEDH, 26 octobre 2000, *Hassan et Tchaouch c/ Bulgarie,* n° 30985/96, § 84).

L'exigence de prévisibilité est d'autant plus nécessaire concernant les textes applicables dans le champ des fichiers de renseignement impliquant une surveillance secrète.

En effet, « *le danger d'arbitraire apparaît avec une netteté singulière là où […] un pouvoir de l'exécutif s'exerce en secret. Puisque l'application de mesures de surveillance secrète échappe au contrôle des intéressés comme du public, la "loi"*

irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire » (CEDH, 6 juin 2006, *Segerstedt-Wiberg c/ Suède*, n° 62332/00, § 76 ; CEDH, 4 mai 2000, *Rotaru c/ Roumanie,* n° 28341/95).

Certes, la Cour admet des restrictions concernant les activités touchant à la sécurité nationale, car « *l'exigence de prévisibilité ne saurait cependant être la même qu'en maints autres domaines. Ainsi, elle ne saurait signifier qu'un individu doit se trouver en mesure d'escompter avec précision les vérifications auxquelles la police […] procédera à son sujet en s'efforçant de protéger la sécurité nationale. Néanmoins, […] la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée* » (CEDH, 26 mars 1987, *Leander c/ Suède*, série A n° 116, § 51).

De sorte qu'il y a violation de l'article 8 lorsque la norme interne ne définit « *ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre* », ne « *fixe pas de limite quant à l'ancienneté des informations détenues et la durée de leur conservation* », et ne contient pas de « *disposition explicite et détaillée sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues* » (CEDH, 4 mai 2000, *Rotaru c/ Roumanie,* n° 28341/95, § 57 ; CEDH, 21 juin 2011, *Shimovolos c/ Russie*, n° 30194/09).

Si la Cour reconnaît une « *certaine latitude* » dans l'interprétation des textes, celle-ci ne doit pas être « *illimitée* » (CEDH, 6 juin 2006, *Segerstedt-Wiberg c/ Suède*, n° 62332/00, § 79).

A cet égard, les dispositions de l'article 26 de la loi Informatique et Libertés, qui autorisent l'absence de publication des arrêtés relatifs à certains fichiers de police, ainsi que les fichiers introduits par ce biais, répondent pas aux exigences posées par la Cour européenne des droits de l'homme, dès lors que les citoyens français n'ont dans cette hypothèse aucune information sur la nature et le contenu des fichiers concernés.

VII. A cela s'ajoute que l'ingérence doit, classiquement, répondre à un « *besoin social impérieux* », reposer sur « *des motifs pertinents et suffisants* » et être « *proportionnée aux buts poursuivis* » (CEDH, 6 juin 2006, *Segerstedt-Wiberg c/ Suède*, n° 62332/00, § 88 ; CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, n°s 30562/04 et 30566/04, § 101 ; CEDH, 18 septembre 2014, *Brunet c/ France*, n° 21010/10, § 33).

Si la Cour ne conteste pas l'intérêt de constituer des fichiers dans le champ de la sécurité, précisant dans son arrêt *S. et Marper* qu'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* » (§ 105), elle examine si les conditions de l'article 8, § 2, sont remplies dans les affaires spécifiques portées à sa connaissance (§ 106).

A cet égard, la Cour a considéré que le FIJAISV poursuivait un objectif légitime de prévention des infractions pénales, dès lors qu'il visait « *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'État, 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* » (CEDH, 17 décembre 2009, *M. B. c/ France,* n° 22115/06, § 54).

Concernant les fichiers des services de renseignement, la Cour rappelle que le pouvoir de surveiller en secret les citoyens n'est tolérable que « *dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* » (CEDH, 6 juin 2006, *Segerstedt-Wiberg c/ Suède*, n° 62332/00, § 88 ; CEDH, 4 mai 2000, *Rotaru c/ Roumanie*, n° 28341/95, § 47), précisant que la conservation d'information dans des fichiers de renseignement poursuit un but légitime, à savoir la défense de l'ordre, la prévention des infractions pénales et la protection de la sécurité nationale (CEDH, 6 juin 2006, *Segerstedt-Wiberg c/ Suède*, n°62332/00, § 87).

VIII. Outre la nécessité, c'est également la proportionnalité de l'ingérence qui est contrôlée. La Cour effectue un contrôle de proportionnalité entre l'atteinte au droit au respect à la vie privée et le but poursuivi, en s'assurant du respect d'un juste équilibre entre les intérêts publics et privés en présence.

A cet égard, elle accorde une certaine marge d'appréciation aux autorités nationales qui, « *grâce à leurs contacts directs et constants avec les forces vives de leur pays, se trouvent en principe mieux placées que le juge international pour se prononcer sur la situation et les besoins locaux* » (CEDH, 18 janvier 2001, *Coster c/ Royaume-Uni*, n° 24876/94, § 105).

Si l'étendue de leurs prérogatives varie en fonction d'un certain nombre de facteurs, comme 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* » (CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, n°s 30562/04 et 30566/04, § 102). Il en va ainsi « *lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu* » (idem).

A cet égard, l'arrêt *S. et Marper* est fondateur s'agissant de l'utilisation des fichiers policiers.

Si la Cour reconnaît que « *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* », elle se doit de procéder à « *un examen rigoureux de toute mesure prise par un État pour autoriser leur conservation et leur utilisation par les autorités sans le consentement de la personne concernée* » (§ 104).

Afin d'évaluer la nécessité de l'ingérence, la Cour considère que la législation interne doit « *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* » (§ 103), cette nécessité se faisant « *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* » (CEDH 18 septembre 2014, *Brunet c/ France*, n° 21010/10, § 35).

Il en ressort qu'un fichage généralisé et illimité dans le temps de la population ne peut se justifier au regard de la jurisprudence de la Cour européenne des droits de l'homme. La conservation des données doit être limitée dans le temps (CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, § 107 ; CEDH, 6 juin 2006, *Segerstedt-Wiberg c/ Suède*, n° 62332/00, § 90), un très long laps de temps ne pouvant être justifié que par « *l'existence de circonstances particulières et par des motifs étayés de manière convaincante* » (CEDH, 18 octobre 2011, *Khelili c/ Suisse*, n° 16188/07, § 63).

Eu égard aux faibles probabilités pour une personne d'obtenir l'effacement des données, la Cour a considéré que la conservation des informations insérées dans le FAED (25 ans) était « *en pratique assimilable à une conservation indéfinie ou du moins, […], à une norme plutôt qu'à un maximum* » (CEDH, 18 avril 2013, *M. K. c/ France*, n° 19522/09, § 45), la même analyse ayant été adoptée pour condamner la France au sujet du système de traitement des infractions constatées (STIC) (CEDH, 18 septembre 2014, *Brunet c/ France*, n° 21010/10, § 43).

Dans cette affaire, la Cour a relevé que le requérant avait bénéficié, à la suite d'une médiation pénale, d'un classement sans suite justifiant qu'il reçoive un traitement différent de celui réservé à une personne condamnée (idem, § 40).

En outre, la Cour vérifie la nature des informations enregistrées et considère que le contrôle qu'elle effectue doit être « *particulièrement attentif aux risques préoccupants de stigmatisation des personnes lorsque celles-ci sont traitées de la même manière que des condamnés, alors même qu'elles n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence* » (CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, § 122 ; CEDH, 18 avril 2013, *M. K. c/ France*, § 36 ; CEDH, 18 septembre 2014, *Brunet c/ France*, § 37).

Or, si « *la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donnent pas l'impression de ne pas être considérés comme innocents* » (CEDH, 18 avril 2013, *M. K. c/ France*, § 36 ; CEDH, 18 septembre 2014, *Brunet c/ France*, § 37). Ainsi, la Cour considère que les durées de conservation des données sur des personnes à l'encontre desquelles n'existent que des soupçons ne devraient pas être aussi longues que celles relatives aux personnes condamnées (CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, § 122).

Par ailleurs, les données enregistrées ne peuvent porter sur une « *allégation très vague et générale* » et qui n'est « *aucunement étayée par des faits concrets* » (CEDH, 18 octobre 2011, *Khelili c/ Suisse*, § 66).

Dans l'arrêt *S. et Marper*, elle a constaté l'absence de juste équilibre entre les droits des personnes fichées et les buts poursuivis, en raison du « *caractère général et indifférencié du pouvoir de conservation en vigueur* » dans le fichier en cause, dès lors que les données en cause pouvaient être « *conservées indéfiniment, quelles que soient la nature et la gravité des infractions dont la personne était à l'origine soupçonnée et indépendamment de son âge, y compris pour des infractions mineures ou non punies d'une peine d'emprisonnement* » (§ 119).

S'agissant du fichier d'empreintes digitales français, la Cour a de la même façon dénoncé le champ d'application trop large des enregistrements possibles, « *susceptible d'englober de facto toutes les infractions, y compris les simples contraventions* » (CEDH, 18 avril 2013, *M. K. c/ France*, § 41), relevant en outre que le droit interne n'opérait « *aucune distinction fondée sur l'existence ou non d'une condamnation par un tribunal, voire même d'une poursuite par le ministère public* » (ibid., § 42).

X. Les exigences européennes en matière de contrôle de proportionnalité sont respectées en droit interne, ainsi que le montre la jurisprudence du Conseil constitutionnel (Cons. const., 22 mars 2012, n° 2012-652 DC ; Cons. const., 13 mars 2014, n° 2014-690 DC ; Cons. const., 27 octobre 2017, n° 2017-670 QPC).

Elles sont également mises en œuvre par le Conseil d'Etat, comme l'illustre la décision *Société HSBC Private Bank* s'agissant d'un fichier des comptes bancaires détenus hors de France par des personnes physiques ou morales (CE, 24 août 2011, n° 336382), la décision *Association pour la promotion de l'image* s'agissant du passeport biométrique (CE, ass., 26 octobre 2011, n° 317827, 317952, 318013 et 318051), la décision *Ligue des droits de l'homme* s'agissant du fichier de traitement des antécédents judiciaires (TAJ) (CE, 11 avril 2014, n° 360759).

Ainsi, par sa décision *Association Aides et autres* (CE, 16 avril 2010, n° 320196), qui a donné lieu à une décision du Conseil constitutionnel (Cons. const., 16 septembre 2010, déc. n° 2010-25 QPC), le Conseil d'Etat s'est conformé à l'arrêt *Bouchacourt c/ France* (CEDH, 17 décembre 2009).

Dans cet arrêt, la Cour juge que l'inscription au fichier national automatisé d'auteurs d'infractions sexuelles fournit les garanties requises, notamment parce que l'effacement des données est de droit, une fois le délai de conservation écoulé (20 ou 30 ans selon la gravité de la condamnation), que la procédure judiciaire d'effacement des données assure un contrôle indépendant de la justification de la conservation des données et que la consultation est exclusivement réservée à des « *autorités astreintes à une obligation de confidentialité et dans des circonstances précisément déterminées* ».

Toutefois, la Cour a conclu à l'inconventionnalité de l'inscription au fichier automatisé des empreintes digitales (CEDH, 18 avril 2013, n° 19522/09, *M. K. c/ France*), au fichier STIC (CEDH, 18 septembre 2014, n° 21010/10, *Brunet c/ France*) et au fichier FNAEG (fichier national automatisé des empreintes génétiques, CEDH, 22 juin 2017, n° 8806/12, *Aycaguer c/ France*) ainsi qu'à l'inconventionnalité de la collecte et la conservation par l'Établissement français du sang de données mentionnant l'orientation sexuelle de la personne (CEDH, 8 septembre 2022, n° 3153/16, *Drelon c/ France*).

Dans l'affaire *Brunet*, le requérant, à la suite d'une plainte déposée par sa concubine, avait été inscrit au fichier STIC et la plainte ayant été classée sans suite, s'était heurté ensuite au refus du procureur de la République de procéder à l'effacement de ses données au fichier.

Pour conclure que la conservation des données au STIC constituait une atteinte disproportionnée au droit au respect de la vie privée du requérant et emporte violation de l'article 8 la Cour a constaté que le requérant ne bénéficiait pas d'un traitement différent de celui réservé à une personne condamnée et encourait un "risque de stigmatisation", que la durée de conservation de la fiche était de vingt ans, que le procureur de la République n'avait pas compétence pour vérifier la pertinence du maintien des informations au STIC et que son contrôle ne saurait passer pour effectif d'autant que sa décision était à l'époque des faits (2009) insusceptible de recours – désormais les décisions du procureur en matière d'effacement ou de rectification relatives à la tenue à jour du STIC peuvent faire l'objet d'un recours pour excès de pouvoir (CE, 17 juillet 2013, n° 359417).

Dans l'affaire *Aycaguer*, le requérant avait été condamné à une peine d'amende de 500 euros pour avoir refusé de se soumettre à un prélèvement biologique en vue de son inscription, sachant qu'il avait été condamné à 2 mois de prison avec sursis pour avoir donné des coups de parapluie à des

gendarmes lors d'une manifestation d'un syndicat agricole. Pour estimer que « *le régime actuel de conservation des profils ADN dans le FAEG [...] n'offre pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante à l'intéressé et ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu* », la Cour a dénoncé trois défaillances dans le FNAEG.

D'abord, la conservation des profils ADN n'offrait pas une protection suffisante car le décret devant aménager la durée maximale de conservation des données (40 ans) n'était pas intervenu.

Ensuite, la procédure d'effacement n'existait que pour les personnes soupçonnées et non pour les personnes condamnées, or ces dernières doivent également pouvoir présenter une requête en effacement des données afin que « *la durée des infractions soit proportionnée à la nature des infractions et aux buts des restrictions* ».

Enfin, aucune différenciation n'était prévue en fonction de la nature et de la gravité de l'infraction commise, malgré la grande disparité des infractions relevant du champ d'application de l'article 706-55 du code de procédure pénale.

X. La Cour européenne des droits de l'homme exerce enfin un contrôle de l'existence de garanties adéquates et suffisantes contre les « *les usages impropres et abusifs* » (CEDH, 4 déc. 2008, *S. et Marper c/ Royaume-Uni*, n°s 30562/04 et 30566/04, § 103 ; CEDH, 18 septembre 2014, *Brunet c/ France*, n° 21010/10, § 35).

La Cour ajoute donc aux « *exigences plutôt négatives contenues dans l'article 8 de la Convention, qui tend pour l'essentiel à prémunir l'individu contre des ingérences arbitraires des pouvoirs publics* », « *des obligations positives inhérentes à un respect effectif de la vie privée* » (CEDH, 19 octobre 2005, *Roche c/ Royaume-Uni*, n° 32555/96, § 157).

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* » (ibid., § 119).

Dans l'arrêt *S. et Marper,* elle a motivé la violation de l'article 8 par le fait qu'il n'existait que peu de possibilités pour un individu acquitté d'obtenir l'effacement des données et que le législateur n'avait pas prévu l'exercice d'un contrôle indépendant de la justification de la conservation.

A cet égard, la Cour exige non seulement que des textes législatifs prévoient un contrôle judiciaire et aménagent des procédures d'effacement, mais en outre que ces garanties soient concrètes et effectives (CEDH, 18 avril 2013, *M. K. c/ France*, n° 19522/09, § 42 ; CEDH, 18 septembre 2014, *Brunet c/ France*, § 36).

Ainsi, si le décret n° 87-249 du 8 avril 1987 relatif au FAED français prévoyait, en cas de refus d'effacement de la part du procureur, la possibilité de saisir le juge des libertés et de la détention, la Cour a estimé que ce droit « *risque de se heurter […] à l'intérêt des services d'enquêtes qui doivent disposer d'un fichier ayant le plus de références possibles […]. 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"* » (CEDH 18 avril 2013, *M. K. c/ France*, § 42).

La réalité du droit à obtenir l'effacement des données peut par ailleurs peser sur l'interprétation de la Cour concernant la durée de conservation des données.

On l'a vu, elle a considéré que la durée de conservation des informations fixée à 25 ans était « *en pratique assimilable à une conservation indéfinie ou du moins, […], à une norme plutôt qu'à un maximum* », « *compte tenu de son précédent constat selon lequel les chances de succès des demandes d'effacement sont pour le moins hypothétiques* » (§ 45).

De même, on l'a vu, elle a condamné la France au sujet du fichier STIC, en relevant que les textes applicables ne donnaient 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'acquittement pour lesquels l'effacement est de principe, mais où il peut prescrire le maintien des données au STIC.

La Cour a considéré qu'il n'avait pas, en l'espèce, 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.

Elle a estimé « *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* » (CEDH, 18 septembre 2014, *Brunet c/ France*, § 41).

Elle a certes pris acte de la jurisprudence récente du Conseil d'État reconnaissant la possibilité d'exercer un recours pour excès de pouvoir contre les décisions du procureur en matière d'effacement ou de rectification, faculté qui n'était toutefois pas reconnue à l'époque des faits. « *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* » (CEDH, 18 septembre 2014, *Brunet c/ France*, § 43).

Enfin, les autorités nationales sont tenues d'offrir aux intéressés une « *procédure effective et accessible* » qui leur permette d'avoir accès à « *l'ensemble des informations pertinentes et appropriées* » (CEDH, 19 octobre 2005, *Roche c/ Royaume-Uni*, § 162 ; CEDH 27 octobre 2009, *Haralambie c/ Roumanie*, n° 21737/03, § 86 ; CEDH, 4 mai 2000, *Rotaru c/ Roumanie*, § 44 ; CEDH, 19 juillet 2011, *Jarnea c/ Roumanie*, n° 41838/05, § 50).

XI. En particulier, dans une affaire *Catt c. Royaume-Uni* (CEDH, 1ère sect., 24 janvier 2019, n° 43514/15), la Cour a proposé une protection inédite des données personnelles ayant trait aux opinions politiques dans les traitements à finalité de renseignement administratif : les informations relatives aux activités militantes et politiques légales d'un activiste non violent constituent des données particulièrement sensibles requérant une protection particulière au titre de l'article 8 et que si leur conservation dans une base à des fins de prévention de l'extrémisme intérieur était possible, elle devait être strictement encadrée et ne pouvait notamment se faire sans limites temporelles.

La doctrine relevait s'agissant de cette affaire que « *le fichier sur lequel reposaient les demandes du requérant avait pour finalité la prévention de « l'extrémisme intérieur » (…). La Cour regrette « la diversité des définitions » que l'on peut donner à ce terme et son « ambiguïté significative » rendant impossible de connaître « le champ exact et le contenu précis » des données collectées (§ 97). Pour autant, et c'est très regrettable, la Cour ne condamne pas fermement cette pratique. Cette question aurait pourtant mérité de plus*

amples développements, ne serait-ce que parce qu'une problématique identique se pose dans beaucoup de pays dont la France à propos des nouveaux textes de procédure pénale spéciale au contenu parfois très obscur (E. Bedarrides, Des écoutes au renseignement : AJDA, 2015, 2026). Le vocabulaire est en droit si fondamental qu'il ne peut se satisfaire de ces mots à géométrie variable et d'une « terminologie trop imprécise », mettait déjà en garde le Doyen Paul Roubier (P. Roubier, Lyon, le 15 novembre 1962 cité par T. Tauran, Le droit et ses théories. Peut-on construire une théorie sur les théories juri- diques : RRJ, 2008, p. 824) » (Droit pénal, n° 6, juin 2019, point n° 116, « Lorsque la Cour européenne des droits de l'homme s'intéresse au fichage des manifestants... échos lointains de débats français »).

Cette décision C*att c. Royaume-Uni* est intéressante à deux égards notamment.

D'une part, sur le caractère individualisé du fichage, la doctrine relevait que « *la Cour énonce un principe très clair, issu d'une recommandation du Comité des ministres (Recomm. N° R (87) 15, 1988, principe 2.4) qu'elle fait sienne : « la collecte de données sur des individus uniquement sur la base de leur participation à des mouvements [...] non interdits par la loi doit être prohibée sauf absolue nécessité » (§ 124). Il n'y a aucune absolue nécessité ici. Plus qu'un détournement de la finalité du fichier,* ***ce que sanctionne la Cour ici est le principe même du fichage d'un individu pour ses seules participations : participer à un groupement politique autorisé ne peut en soi constituer une raison valable du fichage****. Cette solution apparaît éminemment protectrice de la démocratie : chacun est libre de ses activités politiques (DDHC, 26 août 1789, art. 10), tant qu'elles ne sont illicites, et ne peut en être inquiété, même par le biais d'un simple fichier. En France, le principe ainsi énoncé questionne notamment les fichiers PASP (« Prévention des atteintes à la sécurité publique », CSI, art. R. 236-11 et s.) et GIPASP (« Gestion de l'information et de prévention des atteintes à la sécurité publique » : CSI, art. R. 236-21 et s.), qui ont une finalité très proche du fichier anglais (CSI, art. R. 236-11 et 236-21), et dont on ignore quasi tout. Une réflexion similaire se retrouve ensuite quant à la durée de conservation des données* » (idem).

D'autre part, sur la durée limitée du fichage, elle relève que « *la protection de la vie privée ne permet pas une conservation illimitée des données (§ 121). La solution pourrait apparaître classique (CEDH, 4 décembre 2008, n° 30562/04 et 30566/04, S et Marper c/ Royaume-Uni). Pour autant, était bien ici instaurée une période (« minimum ») de six ans, à l'issue de laquelle les données devaient être régulièrement réétudiées, et supprimées si devenues inutiles. L'idée d'une période renouvelable par des actualisations est en effet*

assez séduisante pour les pouvoirs : elle permet de sauvegarder les apparences tout en conservant le plein contrôle sur la durée de conservation. ***La solution est dénoncée par la Cour européenne qui, dans le même souci de réalisme, dénonce un système de maintien des données potentiellement indéfini*** *(§120), d'autant plus que si un recours existe, aucune explication n'est fournie en cas de refus (§ 122), dans le cas du fichier anglais comme des fichiers français (V. par ex. : CE, 27 février 2019, n° 416463, inédit), d'ailleurs. Si le Conseil constitutionnel a en France permis en apparence d'échapper à une telle hypocrisie évidente (Pour le fichier TAJ : Cons. const., 10 mars 2011, n° 2011-625 DC, cons. 72), les fichiers PASP (CSI, art. R. 236- 14) et GIPASP (CSI, art. R. 236-24) adoptent une règle qui, in fine, tend vers le même résultat :* ***la conservation des données pour une durée qui repart à zéro à chaque enregistrement d'un « dernier événement »*** » (idem).

XII. On ajoutera que la Cour de justice de l'Union européenne a repris à son compte l'interprétation de l'article 8 de la CESDH par la Cour européenne relative à la vie privée et à la protection des données à caractère personnel, subordonnant la portée juridique de la législation communautaire (dir. 95/46/CE, 24 octobre 1995 , relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) à la stricte application du droit de la CESDH (CJCE, 20 mai 2003, aff. jointes C-465/00 et C-138/01, *Rechnungshof, Osterreichischer Rundfunk)*.

Il en va de même lorsqu'elle fonde son contrôle sur la Charte des droits fondamentaux de l'Union européenne (art. 7 et 8 ; CJUE, 9 novembre 2010, aff. C-92/09, *Volket und Markus Schecke GbR* ; CJUE, 8 avril 2014, aff. C-293/12, *Digital Rights Ireland*).

Ainsi, c'est de la combinaison de l'article 8 de la CESDH avec les articles 7 et 8 de la Charte que le Conseil d'Etat déduit que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, de données à caractère personnel, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités (CE, Ass., 26 octobre 2011, *Association pour la promotion de l'image et autres,* n° 317827).

XIII. En l'espèce, le décret porte une atteinte disproportionnée au droit au respect de la vie privée et familiale à plusieurs titres.

La protection des données personnelles est d'une importance fondamentale pour la jouissance du droit au respect de la vie privée doit être justifiée par la défense d'un aspect primordial de l'intérêt public et s'accompagner de garanties adéquates et suffisantes, notamment un contrôle judiciaire, contre les abus.

En l'espèce, d'une part, l'ingérence est illégale car la mise en œuvre du fichier ne s'avère ni nécessaire ni proportionné à sa finalité, et, d'autre part, aucune garantie suffisante et adéquate n'est prévue.

Tout d'abord, l'objet du décret ne répond pas à l'exigence de clarté et de prévisibilité, et les finalités du fichier ne sont par conséquent ni déterminées, ni explicites, ni légitimes.

Le décret a pour objet l'« *autorisation de la mise en œuvre par le ministère de l'intérieur (direction générale de la gendarmerie nationale) d'un traitement relatif à la sécurité des établissements, ouvrages, installations et activités nucléaires dénommé « traitement d'optimisation des données et informations d'intérêt nucléaire »* ».

En particulier, aux termes de l'article 1er du décret : « *Au titre de la protection des matières nucléaires, de leurs établissements, ouvrages, installations et des activités nucléaires, à l'exclusion de celles relevant de l'autorité du ministre de la défense en application de l'article R. 1333-3 du code de la défense, contre tout acte de malveillance, le ministre de l'intérieur (direction générale de la gendarmerie nationale) est autorisé à mettre en œuvre un traitement automatisé de données à caractère personnel, dénommé : « traitement d'optimisation des données et informations d'intérêt nucléaire », ayant pour finalités : 1° De faciliter la collecte et l'analyse des informations relatives aux personnes impliquées dans des évènements révélant un risque d'atteinte à la sécurité nucléaire en vue, le cas échéant, de leur diffusion aux autorités compétentes ; 2° De permettre le contrôle et le suivi des demandes d'autorisation d'accès aux établissements, ouvrages, installations impliquant des matières nucléaires ou des sources de rayonnements ionisants et des demandes d'autorisation relatives aux activités de la filière nucléaire. A ce titre, il contribue notamment à la réalisation des enquêtes administratives en assurant la mise en relation avec le traitement de données à caractère personnel dénommé « ACCReD » ; 3° De permettre le traitement et le suivi des demandes d'habilitation mentionnées à l'article R. 2311-7 du code de la défense réalisées au titre de la protection du secret de la défense nationale dans le domaine du nucléaire* ».

Ainsi, la collecte et l'analyse des données personnelles du traitement automatisé litigieux sont justifiées par l'implication de personnes dans des « *évènements révélant un risque d'atteinte à la sécurité nucléaire* ».

Or cette notion, qui n'est à aucun moment définie par le décret, n'est pas assortie des précisions suffisantes.

Si l'on se réfère au Larousse, un événement se définit comme « *tout ce qui se produit, arrive ou apparaît* ».

Cette notion, aux contours flous et élastiques, ne permet pas d'identifier quel comportement peut donner lieu au fichage : il n'est pas précisé quel type d'événement est « *susceptible de porter atteinte à la sécurité nucléaire* » *ou* « *révèle un risque d'atteinte à la sécurité nucléaire* ».

Partant, le périmètre de collecte et d'analyse des données personnelles du traitement automatisé de données est indéterminé, et, par conséquent, illégitime.

En raison de la terminologie très imprécise du décret, le champ des personnes concernées est très étendu – le décret autorisant la collecte et l'analyse des informations des « *personnes impliquées dans des évènements révélant un risque d'atteinte à la sécurité nucléaire* ».

Ainsi, cette disposition permet le traitement automatisé de données personnelles en raison de la participation d'une personne à n'importe quel événement, sans qu'il soit exigé que cette participation ait emporté la commission d'une infraction ou, a fortiori, la condamnation à une sanction.

En particulier, il ressort du texte que l'enregistrement des données personnelles n'est pas soumis à la réalisation d'un risque d'atteinte à la sécurité nucléaire, ni même à un comportement qui serait répréhensible.

Quid de la participation à une manifestation anti-nucléaire ? Quid des actes de militants qui, faisant usage de leur liberté d'expression, alertent précisément sur les risques de l'industrie nucléaire ? Quid des événements passés ?

Or, en matière de traitement automatisé de données personnelles, eu égard aux conséquences que l'utilisation de tels fichiers emportent pour les droits des personnes visées, on ne peut se satisfaire de notions à géométrie variable.

Ensuite, le fichier ne répond à aucune nécessité, de sorte que ses finalités ne justifient pas l'enregistrement de données personnelles si nombreuses et intrusives – on a en précédemment rappelé la teneur.

Ainsi, le décret prévoit un enregistrement de l'ensemble de ces données sur la base des « *implications* » des personnes dans un événement : le principe du fichage est ainsi fondé sur un simple rôle joué, plus ou moins lointain d'ailleurs.

Or, on l'a vu avec l'affaire *Catt* c. *Royaume-Uni*, la Cour européenne des droits de l'homme sanctionne le principe même du fichage d'un individu pour ses seules participations.

Ainsi, à l'instar des fichiers PASP (« Prévention des atteintes à la sécurité publique ») et GIPASP (« Gestion de l'information et de prévention des atteintes à la sécurité publique »), le principe tel qu'énoncé par la Cour européenne des droits de l'homme questionne la nécessité du traitement automatisé prévu par le décret attaqué – ce d'autant plus que les fichiers PASP et GIPASP existent déjà.

Dans ces conditions, l'enregistrement de nombreuses données personnelles sensibles n'est pas justifié par un intérêt public suffisant.

Ainsi l'ingérence dans le droit au respect de la vie privée et familiale des personnes concernées par le *traitement d'optimisation des données et informations d'intérêt nucléaire* apparaît-elle dépourvue de nécessité et donc disproportionnée.

XIV. En outre, le décret ne prévoit pas de garanties adéquates et suffisantes.

D'une part, la période de conservation des données est trop longue et, en ce qu'elle peut être renouvelée à raison de tout nouvel événement révélant un risque d'atteinte à la sécurité nucléaire, doit être regardée comme une durée de conservation indéfinie.

A cet égard, l'article 6 du décret prévoit que : « *Les données à caractère personnel et informations sont conservées :1° S'agissant des données relatives aux personnes physiques impliquées dans des événements susceptibles de porter atteinte à la sécurité nucléaire mentionnées à l'article 2, au maximum cinq ans à compter de la date du* ***dernier événement*** *révélant un risque pour la sécurité nucléaire ayant donné lieu à un enregistrement* ».

On l'a dit, la solution d'une période renouvelable par des actualisations, séduisante pour les autorités nationales en ce qu'elle permet de sauvegarder les apparences tout en conservant le plein contrôle sur la durée de conservation, est dénoncée par la Cour européenne des droits de l'homme qui, dans un souci de réalisme, dénonce un système de maintien des données potentiellement indéfini.

En effet, dans cette configuration, les données sont conservées pour une durée qui repart à zéro à chaque enregistrement d'un « *dernier événement* », autrement dit potentiellement indéfiniment.

D'autre part, le décret prévoit à son article 8 que le droit d'opposition ne s'applique pas au traitement litigieux.

A cet égard, si on sait que le droit d'opposition peut être écarté quand le traitement poursuit un intérêt public, cette exclusion doit être une mesure nécessaire à la finalité poursuivie et il faut mettre en balance l'intérêt public et l'atteinte portée à la vie privée.

En l'espèce en raison de l'imprécision des termes du décret, la finalité du traitement est indéterminée et l'atteinte à la vie privée insuffisamment limitée dans son périmètre, tandis que les données personnelles collectées sont très nombreuses et sensibles.

Ainsi ces personnes, dont les données sont enregistrées en raison de leur implication dans un événement jugé susceptible de porter atteinte à la sécurité nucléaire, se trouvent dans l'impossibilité de savoir si leurs données sont enregistrées, et, partant, de contester cet enregistrement.

D'autant qu'en l'absence de réalisation du risque d'atteinte à la sécurité nucléaire, aucun impératif visant à préserver un intérêt public ne justifie la mise en œuvre du traitement automatisé de données litigieux, alors qu'il existe déjà un traitement automatisé de données à caractère personnel dénommé

« *Prévention des atteintes à la sécurité publique* » ainsi qu'un traitement automatisé de données à caractère personnel dénommé « *Gestion de l'information et prévention des atteintes à la sécurité publique* ».

Enfin, le décret prévoit à son article 9 que les opérations de consultation et de communication sont conservées pendant un délai de trois ans.

Or eu égard à la durée de conservation des données personnelles dans le fichier – à savoir maximum 5 ans, durée renouvelable indéfiniment comme on l'a vu, ce délai de trois ans ne permet manifestement pas de garantir une traçabilité suffisante de l'utilisation des données personnelles par les services y ayant accès.

Dans ces conditions, l'atteinte portée par la mise en œuvre du « *traitement d'optimisation des données et informations d'intérêt nucléaire* » au droit au respect de la vie privée et familiale, garanti par l'article 8 de la CESDH, est disproportionnée.

Le décret encourt donc l'annulation.

XV. Par ailleurs, selon le 1er paragraphe de l'article 10 de la Convention européenne des droits de l'homme, « *toute personne a droit à la liberté d'expression* ».

Il ajoute : « *ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière* ».

Pour la Cour européenne, « *la liberté d'expression constitue l'un des fondements essentiels de la société démocratique, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun* » (CEDH, 7 décembre 1976, *Handsyde* c. *Royaume-Uni*, n°5493/72 ; CEDH, 13 juillet 2012, *Mouvement raëlien suisse* c. *Suisse* [GC], n°16354/06 ; CEDH, 23 avril 2015, *Morice* c. *France* [GC], n°29369/10).

Ainsi, une ingérence dans l'exercice de la liberté d'expression enfreint la Convention si elle ne remplit pas les exigences du paragraphe 2 de l'article 10.

Ce texte prévoit que : « *L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire* ».

Dans la droite ligne de cette liberté d'expression, est également garantie la liberté de manifester, protégée par l'article 11 de la Convention.

On sait, par exemple, que les actions non violentes menées pendant une réunion sont protégées par ce texte, ce qui est le cas de barrages routiers et d'autres comportements physiques visant délibérément à bloquer la circulation routière et à entraver le bon déroulement de la vie quotidienne (CEDH, 5 mars 2009, *Baracco c. France*, n° 31684/05).

Relève de la protection de l'article 10 ou des articles 10 et 11 combinés, les actes visant à entraver des activités d'une nature donnée, tels que des actes de protestation destinés à empêcher physiquement une chasse ou la construction d'une autoroute (CEDH, 23 septembre 1998, n° 67/1997).

Les États doivent non seulement s'abstenir d'apporter des restrictions indirectes abusives au droit de réunion pacifique mais également protéger ce droit.

La liberté d'expression est, en outre, protégée, en droit interne, par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 : « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* ».

Pour le Conseil constitutionnel, « *la liberté d'expression et de communication, dont découle le droit d'expression collective des idées et des opinions, est d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés* », de sorte que « *les atteintes portées à l'exercice de cette liberté et de ce droit doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi* » (Cons. const., 4 avril 2019, n° 2019-780 DC, § 8).

Il rappelle : « *il appartient au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et libertés constitutionnellement garantis, au nombre desquels figurent [notamment] le droit d'expression collective des idées et des opinions* » (§ 9).

Et il a jugé que porte une atteinte disproportionnée au droit d'expression collective des idées l'interdiction de manifester, prononcée par l'autorité administrative, sur le fondement de tout agissement, que celui-ci ait ou non un lien avec la commission de violences et ce, quelle que soit son ancienneté, ce qui laisse à l'autorité administrative une latitude excessive dans l'appréciation des motifs susceptibles de justifier l'interdiction (§ 23).

Or, en raison – on insiste, mais c'est important – de l'absence de définition précise des comportements donnant lieu à une inscription au fichier ODIINUC, le simple risque d'une telle inscription pour les militants opposés à l'industrie du nucléaire est de nature à décourager – et donc à entraver purement et simplement – l'exercice de leur liberté d'expression, notamment sous sa forme collective.

Et aucun impératif de sécurité publique ne peut justifier une telle atteinte, laquelle se révèle disproportionnée, en méconnaissance des articles 10 et 11 de la Convention européenne des droits de l'homme.

Pour toutes ces raisons, le décret devra être annulé.

PAR CES MOTIFS et tous autres à produire, déduire ou suppléer, au besoin même d'office, les exposants concluent qu'il plaise au Conseil d'Etat :

- ANNULER le décret attaqué ;

- METTRE A LA CHARGE de l'Etat la somme de 6 000 € en application des dispositions de l'article L. 761-1 du code de justice administrative.

SAS Zribi & Texier
Avocat aux Conseils

PRODUCTIONS :