Anne SEVAUX et Paul MATHONNET
Société Civile Professionnelle
AVOCAT AU CONSEIL D'ETAT
ET A LA COUR DE CASSATION
12, rue de Bourgogne, 75007 PARIS
tél : 01.43.17.39.00
fax : 01.43.17.39.09
cabinet@as-pm.fr

CONSEIL D'ETAT

Section du Contentieux

RECOURS POUR EXCES DE POUVOIR
REQUETE ET MEMOIRE

POUR : **La Confédération Générale du Travail**, dont le siège se trouve 263, rue de Paris 93516 Montreuil Cedex, représentée par son représentant légal en exercice, domiciliée audit siège ;

La Confédération Générale du Travail – Force ouvrière dont le siège se trouve 141, avenue du Maine 75014 Paris, représentée par son représentant légal en exercice, domiciliée audit siège ;

La Fédération syndicale unitaire, dont le siège se trouve 104, rue Romain Rolland 93260 Les Lilas, représentée par son représentant légal en exercice, domiciliée audit siège ;

L'Union syndicale Solidaires, dont le siège se trouve 31, rue de la Grange aux belles 75010 Paris, représentée par son représentant légal en exercice, domicilié audit siège ;

Le Syndicat de la magistrature, dont le siège situé 91, rue de Charenton, 75012 Paris, représenté par sa présidente en exercice, domiciliée audit siège ;

Le Syndicat des avocats de France, dont le siège situé 34 rue Saint Lazare 75009 Paris, représenté par sa présidente en exercice, domiciliée audit siège ;

Le Groupe d'information et de soutien des immigré·e·s (Gisti), dont le siège se trouve 3, villa Marcès, 75 011 Paris, représentée par sa présidente en exercice, domiciliée audit siège ;

L'Union nationale des étudiants de France, dont le siège se trouve 127, rue de l'Ourcq 75019 Paris, représentée par sa présidente en exercice, domiciliée audit siège ;

demandeurs,
S.C.P. Anne SEVAUX et Paul MATHONNET,

CONTRE : Le décret n° 2020-1510 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique» (**EASP**)(**production n°1**).

FAITS ET PROCEDURE

1. En 2008, le gouvernement a décidé de supprimer le «fichier alphabétique des renseignements», qui comprenait 60 millions de fiches impliquant 20 millions de personnes, en raison de sa non-conformité aux exigences de la loi informatique et liberté et de ses insuffisances techniques.

Pour le remplacer, il a développé le projet Edvige qui consistait à reprendre dans un traitement automatisé une partie des données contenues dans les fichiers des renseignements généraux.

Créé par un décret du 27 juin 2008, le fichier Edvige ouvrait la possibilité d'enregistrer des données sensibles telles que celles portant sur les opinions politiques, philosophiques et religieuses ou l'appartenance syndicale ou des données relatives à la santé ou à la vie sexuelle. Le mouvement de protestation qu'il a suscité a conduit à son retrait par le décret n° 2008-1199 du 19 novembre 2008.

Après le retrait du décret Edvige, le gouvernement a pris le parti de renoncer à l'enregistrement de données relatives aux personnalités et a élaboré un projet limité à deux finalités que sont la prévention des atteintes à l'ordre public et la réalisation des enquêtes administratives.

C'est ainsi qu'ont été créés, par le décret n° 2009-1249, le fichier de prévention des atteintes à la sécurité publique (PASP) et, par le décret n° 2009-1450, le fichier des enquêtes administratives liées à la sécurité publique (EASP).

2. Le fichier « EASP », placé sous la responsabilité du ministère de l'intérieur (direction centrale de la sécurité publique et préfecture de police), a pour objet de faciliter la réalisation des enquêtes administratives conduites en application des articles des articles L. 114-1, L. 114-2 et L. 211-11-1 du présent code et de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

Plus précisément, ce traitement vise à assurer la fiabilité d'enquêtes effectuées par le recoupement au niveau national d'informations collectées, archivées et exploitées pour répondre aux demandes d'enquêtes administratives, dans le but de déterminer si le comportement de l'intéressé est ou non compatible avec l'exercice des fonctions ou des missions envisagées.

Les règles applicables au traitement des données collectées dans ce fichier sont régies par les dispositions codifiées aux articles R. 236-1 à R. 236-10 du code de la sécurité intérieure, dont il résulte que sont autorisés à accéder aux données qu'il contient, non seulement les agents affectés dans les services du renseignement territorial, mais également les agents habilités des services nationaux « des enquêtes administratives de sécurité » et de « Commandement spécialisé pour la sécurité nucléaire », ainsi que tout autre agent d'une unité de la gendarmerie nationale ou d'un service de la police nationale, sur demande expresse.

Ce fichier figure au nombre des fichiers que les pouvoirs publics peuvent, par l'intermédiaire du fichier ACCReD consulter automatiquement et simultanément.

Selon le ministère de l'intérieur, 221 711 individus étaient recensés dans le fichier « EASP » au mois de novembre 2020.

3. Entre temps, trois rapports rédigés pour le compte de l'Assemblée nationale ont tous pointé du doigt la confusion entretenue par la multiplicité des fichiers et la faiblesse des garanties apportées à la protection des données personnelles (rapport d'information n°1548 sur les fichiers de police enregistré le 24 mars 2009 ; rapport d'information n°4113 sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police enregistré le 21 décembre 2011 ; rapport d'information n°1335 sur les fichiers mis à disposition des forces de sécurité enregistré le 17 octobre 2018).

Ces rapports ont ainsi mis en lumière la multiplication des fichiers de police (106 fichiers recensés à la date du 17 octobre 2018), l'inutilité d'une partie d'entre eux (25% d'entre eux en 2011), et surtout le caractère « clandestin » de nombre de fichiers dépourvus de base légale et non déclarés (45% d'entre eux en 2011).

S'agissant en particulier de la gendarmerie nationale, la DGGN est responsable de 44 traitements qui comprennent notamment des logiciels de

rédaction des procédures, de gestion des gardes à vue, de diffusion et de partage d'informations opérationnelles ou des logiciels de rapprochements judiciaires.

4. C'est dans un contexte marqué par une circonspection certaine vis-à-vis des fichiers de police et de gendarmerie que le Premier ministre a d'abord, par un décret n° 2020-151 du 20 février 2020, autorisé le traitement automatisé de données dit «GendNotes» sur tablette comportant une zone de commentaires libres permettant aux gendarmes de collecter des données relatives à la prétendue origine raciale ou ethnique, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale, à la santé, à la vie sexuelle ou à l'orientation sexuelle.

Un recours formé contre ce décret est actuellement pendant (n° 442307).

Puis, le Premier ministre a décidé de modifier le régime des fichiers GIPASP et PASP en ajoutant à leur finalité initiale, qui consistait dans le traitement de données relatives aux personnes susceptibles d'être impliquées dans des actions de violence collectives en particulier en milieu urbain ou à l'occasion de manifestations sportives, une nouvelle finalité consistant dans le traitement de données les personnes susceptibles de prendre part à des activités terroristes, de porter atteinte à l'intégrité du territoire ou des institutions de la République, au titre de la sûreté de l'Etat

Il a également décidé de modifier le fichier « EASP » en élargissant considérablement les catégories de données susceptibles d'être collectées afin qu'il intègre désormais les données intéressant la sûreté de l'Etat.

En raison de la nature des données qu'il est susceptible de collecter et de mémoriser, le projet de décret modifiant les dispositions du code de la sécurité intérieure relatives au traitement «EASP» a été soumis à la consultation préalable de la CNIL qui a émis à son sujet une délibération n° 2020-066 en date du 25 juin 2020 formulant des recommandations qui n'ont pas toutes été suivies (**production n°2**).

Par un décret en Conseil d'Etat n° 2020-1510 du 2 décembre 2020, le Premier ministre a modifié les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé «Enquêtes administratives liées à la sécurité publique» ou «EASP» (**production n°1**).

5. De manière générale, les modifications consistent à élargir les données enregistrées par le traitement qui collectait initialement le motif de l'enquête, les informations ayant trait à l'état civil, les photographies, les titres d'identité, ainsi que le rapport de l'enquête administrative, contenant les éléments permettant de déterminer si le comportement de la personne concernée n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées, compte tenu de leur nature.

L'article 1er du décret ajoute à ces données celles « *intéressant la sûreté de l'Etat* », c'est-à-dire « *celles qui révèlent des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts. Ces données, de façon isolée ou groupée, font l'objet d'une identification dans le traitement* ».

L'article 2 précise la nature des données susceptibles d'être collectées et énonce ainsi 50 catégories de données, au nombre desquelles figurent notamment les activités publiques ou au sein de groupements ou de personnes morales, les comportements et habitudes de vie, les déplacements, les activités sur les réseaux sociaux, les données relatives aux troubles psychologiques ou psychiatriques, obtenues conformément aux dispositions législatives et réglementaires en vigueur, les pratiques sportives, les pratiques et comportements religieux, les facteurs de fragilité, les facteurs sociaux et économiques, les faits dont la personne a été victime, le comportement auto-agressif, ou l'indication de l'enregistrement ou non de la personne dans une série de traitements de données à caractère personnel.

Mais ce n'est pas tout, car l'article 3 ajoute que l'enregistrement de données, contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des fonctions est autorisé alors même que ce comportement tiendrait à la dangerosité que feraient apparaitre les données, relatives aux troubles psychologiques ou psychiatriques de l'intéressé, étant entendu que ces dispositions prévoyaient déjà l'enregistrement de données relatives à un comportement incompatible avec l'exercice des fonctions lorsque ce comportement aurait une motivation politique, religieuse, philosophique ou syndicale.

L'article 6 tire les conséquences de ces modifications et prévoit que s'agissant des données intéressant la sûreté de l'Etat, les droits d'accès, de rectification et d'effacement s'exercent devant la CNIL en application des dispositions spécifiques applicables aux traitements concernant la sûreté de l'Etat.

6. Ce décret n° 2020-1510 du 2 décembre 2020 est la décision attaquée.

DISCUSSION

I] Sur l'intérêt à agir des requérants

7. En leur qualité de personne morale, syndicats ou associations, les exposants disposent d'un intérêt propre à agir contre le décret attaqué dans la mesure où le décret attaqué autorise d'abord la collecte de données relatives aux « *activités publiques ou au sein de groupement ou de personnes morales* » (soulignement ajouté).

En permettant ainsi la collecte de données relatives d'une part aux activités publiques et, d'autre part, aux activités au sein de groupements ou de personnes morales, le décret vise ici toutes les personnes qui auraient adhéré à une association ou à un syndicat et qui, en tant qu'adhérant, y exercerait une activité, que celle-ci revêt ou non un caractère public.

Pour ce premier motif, le décret affecte directement les membres des syndicats ou associations exposants qui exercent en leur sein une activité quelle qu'elle soit.

8. En outre, la Confédération générale du travail, la Confédération générale du travail -Force Ouvrière, la Fédération syndicale unitaire, l'Union syndicale Solidaires, le Syndicat de la magistrature, le Syndicat des avocats de France et l'UNEF ont tous pour objet statutaire de défendre les droits et intérêts professionnels, moraux et matériels, sociaux et économiques, individuels et collectifs de leur membres, de promouvoir un syndicalisme unitaire et indépendant, démocratique et pluraliste, au service des aspirations et des revendications des personnels qu'elle regroupe, ainsi que la liberté syndicale.

D'une part, en tant que le décret modifie et élargit l'accès à un traitement qui est susceptible de collecter des données relatives aux opinions politiques, religieuses, philosophiques ou syndicales, il affecte l'intérêt de leurs membres par le caractère discriminant et stigmatisant de cette collecte.

A cet égard, il doit être précisé que la Confédération générale du travail, le Syndicat de la Magistrature, le Syndicat des avocats de France ont par ailleurs déjà formé des recours contre les dispositions réglementaires instituant un traitement automatisé relatif aux modalités d'évaluation de personnes se déclarant mineures et celles créant le fichier dit «Edvige», lesquels ont été rejetés au fond sans que l'intérêt à agir de ces syndicats n'ait été remis en cause (CE, Ord., 3 avril 2019, n° 428477 ; CE, Ord., 29 octobre 2008, n° 321413).

D'autre part, en tant que le décret étend considérablement la nature des données susceptibles d'être recueillies dans le cadre et pour la réalisation des enquêtes administratives, il porte directement atteinte aux intérêts professionnels des membres des unions, fédérations et syndicats exposants.

On le sait, l'accès à un grand nombre de fonctions et de responsabilité susceptibles d'être confiées aux agents publics comme aux salariés est soumis à la réalisation d'une enquête administrative.

Il en va par exemple ainsi des décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation, 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.

Il en va également des décisions de recrutement et d'affectation concernant les emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes ou d'une entreprise de transport de marchandises dangereuses soumise à l'obligation d'adopter un plan de sûreté peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées.

Dans la mesure où les données collectées en vertu de ce décret sont susceptibles d'être opposées aux salariés et agents publics qui prétendraient à l'exercice de ces fonctions ou de ces responsabilités pour rejeter leur demande, les dispositions attaquées portent atteinte à leurs intérêts professionnels.

Partant, ces dispositions affectent donc directement l'intérêt collectif que la CGT, la CGT-FO, la FSU, Solidaires, le Syndicat de la Magistrature, le SAF et l'UNEF entendent défendre.

9. A ceci s'ajoute la circonstance que les intérêts du Syndicat de la magistrature et du Syndicat des avocats de France sont directement affectés à raison des conditions d'exercice de la profession qu'ils entendent chacun défendre.

D'une part, l'accès à la magistrature est soumis à la réalisation d'une enquête administrative, de sorte que l'élève de l'école nationale de la magistrature dont les données seront collectées dans le fichier litigieux à raison du décret attaqué pourra se les voir opposer en cas de refus d'accès à la magistrature.

Le décret affecte donc directement l'intérêt collectif que le Syndicat de la magistrature s'est donné pour mission de défendre.

D'autre part, dans la mesure où le traitement automatisé de données modifié par le décret attaqué constitue un outil à disposition des membres de la police et de la gendarmerie nationale agissant, notamment, dans le cadre de procédures judiciaires, les droits des justiciables que les avocats sont amenés à défendre, à la date de la collecte des données ou de leur utilisation, s'en trouvent directement affectés. L'enregistrement et la collecte d'informations sensibles, tenant notamment à des données subjectives comme celles qui ont trait à l'état de santé, ou aux opinions ou à l'appartenance religieuse, ou à l'état de santé, peuvent en effet affecter, par leur caractère discriminant, la capacité des personnes intéressées et de leur avocat à exercer leurs droits de la défense.

L'enregistrement de données sensibles, allant jusqu'à des données relatives aux opinions politiques, philosophiques, religieuses ou à des données de santé révélant une dangerosité particulière, ceci sans le moindre encadrement, affecte par ailleurs les libertés publiques et individuelles en faveur desquelles le syndicat des avocats de France s'est donné pour mission d'œuvrer.

10. Il faut encore ajouter que l'association GISTI dispose également d'un intérêt particulier à agir en tant que le décret attaqué affecte l'intérêt des catégories de populations que cette association défend.

D'abord, l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, visé par l'article R. 236-1 du code de la sécurité intérieure, soumet les demandes d'acquisition de la nationalité française et de délivrance de titres de séjour donnent lieu à une consultation des traitements automatisés de données à caractère personnel et en particulier du fichier litigieux.

Ensuite, l'article L. 114-1 du code de la sécurité intérieure, visé par l'article R. 236-1 du même code, prévoit qu'il peut être procédé à une enquête administrative pour la délivrance, le renouvellement ou le retrait d'un titre ou d'une autorisation de séjour sur le fondement des articles L. 121-4, L. 122-1, L. 311-12, L. 313-3, L. 314-3 et L. 316-1-1 du code de l'entrée et du séjour des étrangers et du droit d'asile ou des stipulations équivalentes des conventions internationales ainsi que pour l'application des articles L. 411-6, L. 711-6, L. 712-2 et L. 712-3 du même code.

Dans les deux cas, l'étranger qui sollicite un titre de séjour ou l'acquisition de la nationalité française ou qui se voit retirer un titre sur le fondement des dispositions précitées, peut se voir opposer des données recueillies dans le traitement litigieux en application du décret attaqué.

Or, en tant qu'il élargit considérablement l'étendue des données susceptibles d'être collectées et enregistrées, et susceptibles de leur être opposées, le décret attaqué porte gravement atteinte aux droits des personnes de nationalité étrangères.

Enfin, le fichier litigieux a vocation à collecter les données relatives à la régularité du séjour des individus et cette catégorie de donnée sera collectée, ainsi que l'a relevé la CNIL, à la faveur d'un rapprochement manuel avec d'autres fichiers. Ce rapprochement manuel est de nature à entraîner une saisie des informations qui peut être erronée parce que réalisée pour un homonyme, parce que non correctement reportée ou parce que l'auteur de la saisie ne s'est pas assurée de ce que l'information reportée n'est pas depuis lors devenue obsolète. En outre, l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, visé par l'article R. 236-

1 du code de la sécurité intérieure, soumet les demandes d'acquisition de la nationalité française et de délivrance de titres de séjour à une consultation.

Le décret affecte donc directement l'intérêt collectif des personnes de nationalité étrangère que le GISTI s'est donné pour mission de défendre.

La recevabilité de la requête est donc acquise.

II] Sur l'illégalité du décret

A] Sur l'illégalité externe du décret faute pour le décret d'avoir été précédé d'une consultation régulière du Conseil d'Etat

11. Il résulte par ailleurs de la loi du 6 janvier 1978 que la CNIL «*est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données* ».

Le décret définitivement adopté doit être conforme au projet de décret soumis par le Gouvernement à la consultation de la section de l'intérieur du Conseil d'Etat, et, *a fortiori*, à la minute de la section du Conseil d'Etat qui l'a examiné.

Si tel n'est pas le cas, il est acquis que le décret a été pris au terme d'une procédure irrégulière (pour un exemple récent d'annulation : CE, 5 février 2020, *UNICEF France,* n° 428478 ; voir également : CE, 24 octobre 2019, *Fédération des transports et de la logistique FO-UNCP*, n° 422583 ; CE, 20 décembre 2013, n° 357198, publié au Lebon ; CE, 10 janvier 2007, *Fédération nationale interprofessionnelle des mutuelles,* n° 283175, mentionné aux tables).

20. En l'état, à défaut de toute justification utile et contradictoire permettant de s'assurer que le décret attaqué est conforme au projet de décret soumis par le gouvernement au Conseil d'Etat, ou à la minute de la section du Conseil d'Etat qui l'a examiné, l'irrégularité devra être constatée.

En l'absence de consultation régulière du Conseil d'Etat, le décret attaqué est entaché d'incompétence.

L'annulation est encourue.

B] **<u>Sur l'illégalité interne du décret</u>**

12. Ses dispositions seront regardées comme entachées d'illégalité en tant qu'elles portent une atteinte disproportionnée au droit au respect de la vie privé et à la liberté de pensée, de conscience et de religion (**B.1**), et en tant qu'elles méconnaissent l'article 4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (**B.2**).

Son illégalité sera en outre constatée du fait de la contrariété des dispositions avec les dispositions de l'article 88 de cette même loi du 6 janvier 1978 (**B.3.**).

B.1.] **Sur la violation du droit au respect de la vie privée, de la liberté de pensée, de croyance et de religion à raison de l'absence de finalité claire et légitime donnée au traitement litigieux, du caractère inadéquat et non pertinent des données collectées, du périmètre excessivement étendu de l'accès aux données et de la durée excessive de conservation des données**

13. La collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel portent atteinte au droit au respect de la vie privée tel qu'il est consacré par l'article 2 de la déclaration des

droits de l'homme et du citoyen (Cons. Const., 22 mars 2012, décision n° 2012-652 DC, loi relative à la protection de l'identité, cons. 8 ; Cons. Const., 11 mai 2020, n° 2020-800 DC, loi prorogeant l'état d'urgence sanitaire, cons. 61).

L'atteinte qui en résulte n'est regardée comme étant proportionnée que lorsque le traitement automatisé est justifié par un motif d'intérêt général et que sa mise en œuvre est adéquate et proportionnée à cet objectif (Cons. Const., 22 mars 2012, décision n° 2012-652 DC, loi relative à la protection de l'identité, cons. 8 ; Cons. Const., 11 mai 2020, n° 2020-800 DC, loi prorogeant l'état d'urgence sanitaire, cons. 61).

Dans le même sens, la Cour européenne des droits de l'homme juge que les éléments relatifs à l'identité de l'individu, à son orientation sexuelle ou à son identité ethnique relèvent du droit au respect de la vie privée et que la mémorisation de ces données constitue une ingérence au sens de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Unis*, §62 ; CEDH, 18 octobre 2011, *Khelili c. Suisse*, n° 16188/07, §55 ; CEDH, 18 septembre 2014, *Brunet c. France*, n°21017/10, §35 ; CEDH, 22 juin 2017, *Aycaguer c. France*, n° 8806/12, §33).

Elle ne considère l'ingérence comme justifiée que lorsque le droit interne contient des exigences détaillées quant à l'utilisation du traitement, l'accès des tiers, des procédures destinées à ce que les justiciables disposent de garanties suffisantes et aptes à les protéger efficacement des usages impropres et abusifs, que le but poursuivi est légitime, et que les données recueillies sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées (CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Unis*, §101 ; CEDH, 18 octobre 2011, *Khelili c. Suisse*, n° 16188/07, §60 ; CEDH, 18 septembre 2014, *Brunet c. France*, n°21017/10, §36 ; CEDH, 22 juin 2017, *Aycaguer c. France*, n° 8806/12, §34).

L'intérêt de l'Etat défendeur à la protection de la sécurité nationale et de la sûreté nationale doit être mis en balance avec la gravité de l'ingérence dans l'exercice par les requérants respectifs de leur droit au respect de leur vie privée et la Cour européenne des droits de l'homme juge de ce fait que la conservation d'informations relatives à la participation à une réunion politique ne se fonde pas sur des motifs pertinents et suffisants au regard de la protection de la sécurité nationale compte tenu de la nature de ces renseignements (CEDH, 6 juin 2006, *Segerstedt-Wibert et a. c. Suède*, n°323332/00, §90).

Le traitement des données personnelles relatives aux opinions et aux convictions qu'elles soient politiques, sociales, philosophiques, syndicales ou religieuses est par ailleurs de nature à porter atteinte à la liberté de pensée, de conscience et de religion consacrée par les dispositions de l'article 10 de la Déclaration des droits de l'homme et du citoyen, celles de l'article 10 de la Charte des droits fondamentaux de l'Union européenne, et par les stipulations de l'article 11 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (v. en ce sens : A. BRETONNEAU, concl. lues sous : CE, 11 juillet 2018, *Ligue des droits de l'Homme*, n°414827).

En effet, le corollaire de la liberté de pensée, de conscience et de religion réside dans la garantie de chaque individu de ne pas être inquiété à raison de ses opinions et de ses croyances, et cette garantie est nécessairement remise en cause par la collecte de données relatives aux opinions, convictions ou croyances religieuses puisqu'elle conduit à admettre que les autorités publiques peuvent prendre des actes ou des décisions sur la base de celles-ci.

Partant, la collecte des données relatives à l'identité des individus et à leurs opinions politiques, philosophiques, syndicales, religieuses constitue en elle-même une atteinte au droit au respect à la vie privée et familiale d'une part, et au droit à la liberté de pensée, de conscience et de religion d'autre part.

14. Ces principes étant posés, la législation répartit les traitements de données à caractère personnel en trois catégories.

La grande majorité des traitements est soumise au règlement européen général sur la protection des données personnelles n° 2016/679 du 27 avril 2016 précisé et complété par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Ceux réalisés à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, relèvent de la directive européenne dite « police-justice » du 27 avril 2016 et des dispositions du titre III de la loi n°78-17 du 6 janvier 1978 qui la transposent.

Enfin, une dernière catégorie de traitements qui intéresse la sûreté nationale et la défense nationale n'est pas soumise au droit de l'Union mais aux seules dispositions spécifiques de la loi n°78-17 du 6 janvier 1978.

Comme tous ont en commun de constituer une mesure entraînant une ingérence dans l'exercice du droit de toute personne au respect de sa vie privée, l'article 4 de la loi n°78-17 du 6 janvier 1978 pose une triple exigence d'adéquation, de pertinence et de limitation du traitement et des données collectées à ce qui est strictement nécessaire.

Le Conseil d'Etat juge à ce titre que la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives constituent une ingérence dans l'exercice du droit de toute personne au respect de sa vie privée, et que cette ingérence ne peut être légalement autorisée que si elle répond à des finalités légitimes et si 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*, n° 317827, publié au Lebon).

Ce contrôle n'est pas réalisé de manière globale mais est successivement appliqué aux différentes caractéristiques du fichier, c'est-à-dire à la finalité poursuivie, aux données recueillies, au périmètre des destinataires et à la durée de conservation des données.

15. Le vecteur principal est la finalité poursuivie puisque c'est au regard de celle-ci que la pertinence des durées collectées sera appréciées, de même que l'étendue des destinataires des données ou leur durée de conservation.

C'est en effet au regard de la finalité du traitement que sera déterminé le cadre juridique applicable : le traitement de données intéressant la sûreté de l'Etat est ainsi exclue du champ d'application de la directive 2016/680 et relèvent spécifiquement des articles 1 à 41 et 115 à 124 de la loi du 6 janvier 1978, à la différence des données recueillies pour répondre à une finalité étrangère aux atteintes à la sûreté de l'Etat (v. en ce sens : CE, 27 mars 2020, *CRPA*, n° 431350, mentionné aux tables).

C'est également au regard de la finalité du traitement telle qu'elle est énoncée par l'acte l'autorisant que le juge contrôle la pertinence du périmètre des données collectées, l'étendue des personnes bénéficiaires des données et le caractère limité de la durée de leur conservation (V. A. LALLET, concl. lues sous : CE, 27 mars 2020, n° 317182 ; v. également : CE, 30 décembre 2009, n° 312051, publié au Lebon ; CE, 11 mars 2011, n° 332886 ; 21 septembre 2015, *association de défense et d'assistance juridique des intérêts des supporters et*

autres, n°389815, mentionné aux tables ; CE, 11 juillet 2018, *Ligue des droits de l'homme*, n° 414827).

Et, c'est enfin au regard de cette finalité que sera apprécié le caractère proportionné de l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée : le renseignement pour la sûreté de l'Etat justifiera la collecte de données plus sensibles et dont la conservation sera plus longue là que les données collectées pour le renseignement tendant à faciliter la caractérisation d'infractions.

16. Dans le cas présent, pour mémoire, l' «EASP» a, à l'origine, pour unique finalité « *de faciliter la réalisation d'enquêtes administratives (...) par la conservation des données issues de précédentes enquêtes relatives à la même personne.* »

L'article premier du décret attaqué a modifié l'article R. 236-1 du code de sécurité intérieure pour ajouter une mention relative à la sûreté de l'Etat, de sorte que cet article dispose désormais :

> « *Le ministre de l'intérieur (direction centrale de la sécurité publique et préfecture de police) est autorisé à mettre en œuvre un traitement automatisé de données à caractère personnel dénommé " Enquêtes administratives liées à la sécurité publique ", ayant pour finalité de faciliter la réalisation d'enquêtes administratives en application des articles L. 114-1, L. 114-2 et L. 211-11-1 du présent code et de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité par la conservation des données issues de précédentes enquêtes relatives à la même personne y compris celles intéressant la sûreté de l'Etat.*
> *Les données intéressant la sûreté de l'Etat sont celles qui révèlent des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts. Ces données, de façon isolée ou groupée, font l'objet d'une identification dans le traitement.».*

La finalité assignée à ce traitement n'a pas été modifiée par le décret puisqu'elle a toujours pour objet de « *faciliter la réalisation d'enquête administrative* » « *par la conservation des données issues de précédentes enquêtes relatives à la même personnes* ». Tout au plus, le décret ajoute une précision quant à l'étendue de ces données puisqu'il précise « *y compris celles intéressant la sûreté de l'Etat* ».

Il vient ainsi uniquement préciser que les données conservées à l'issue de précédentes enquêtes administratives relatives à la même personne pourront concerner des données intéressant la sûreté de l'Etat, c'est-à-dire les données intéressant par exemple le niveau de radicalisation d'un individu, les liens avec des groupes extrémistes ou la détention d'armes.

La circonstance que le décret ajoute à ces dispositions les données intéressant la sûreté de l'Etat n'a donc pas pour objet ni pour effet de modifier la finalité poursuivie par le traitement qui demeure la facilitation de la réalisation des enquêtes administratives par la conservation des données issues de précédentes enquêtes relatives à la même personne.

Compte tenu de la finalité poursuivie, il sera démontré que le décret attaqué emporte une atteinte manifestement disproportionnée au droit au respect de la vie privée et à la liberté d'opinion, de conscience et de religion qui n'est ni nécessaire ni proportionnée au regard de :

- du caractère inadéquat et non pertinent des données collectées (**B.1.1.**)
- du périmètre excessivement étendu de l'accès aux données (**B.1.2.**)
- du caractère excessif de la durée de conservation des données (**B.1.3.**).

B.1.1. Sur le caractère inadéquat et non pertinent des données collectées

17. Tout traitement, quelles que soient les données traitées, est soumis aux règles générales posées par l'article 4 de la loi n°78-17 du 6 janvier 1978 dont il résulte que les données collectées sont soumises à une triple exigence qui consiste dans l'adéquation, la pertinence et le caractère non excessif des données au regard des finalités pour lesquelles elles sont traitées.

Cette triple exigence est appréciée qualitativement et quantitativement.

18. Sous l'angle quantitatif d'abord, la jurisprudence administrative et constitutionnelle exige que, au regard de leur nature, les données recueillies

soit limitées, car de cette limitation dépend le nombre de personnes susceptibles d'être concernées par la collecte (V. A. LALLET, concl. lues sous : CE, 27 mars 2020, n° 317182 ; v. également : CE, 30 décembre 2009, n° 312051, publié au Lebon ; CE, 11 mars 2011, n° 332886).

Pour ce motif, ont été censurés le traitement biométrique qui comprenait des données très sensibles susceptibles de concerner la quasi-totalité de la population française (Cons. Const. 22 mars 2012, décision n°2012-652, loi relative à la protection de l'identité, cons. n°10), comme celui relatif à la gestion du suivi des affaires pénales par le parquet général en tant qu'il intégrait les données des personnes mises en cause dans une enquête préliminaire ou de flagrance alors même qu'elles n'étaient pas nécessairement appelées à être des parties à un litige devant une juridiction d'instruction ou de jugement (CE, 24 janvier 2001, n°212484, publié au Lebon).

Dans la même ligne, la Cour de Strasbourg a censuré le fichier FAED dont le périmètre était trop extensif, puisque susceptible d'englober de facto les données relatives à toutes les infractions sans distinction (CEDH, 18 avril 2013, *M. K. c. France*, n° 19522/09, §41).

Ces considérations ont d'ailleurs conduit à préconiser l'interdiction de la collecte des données sensibles dans le cadre des missions d'enquête administrative et la limitation des données collectées à un nombre restreint d'individus (rapport d'information n°4113 sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police enregistré le 21 décembre 2011, pages 48 et 58 ; v. également en ce sens : CEDH, 4 mai 2000, *Rotaru c. Roumanie,* n°28341/95, §34).

Il appartient ainsi au pouvoir réglementaire de déterminer les catégories de données qui peuvent être collectées en lien direct avec le motif d'enregistrement afin de limiter le périmètre des personnes concernées afin de garantir un rapport direct entre la collecte de donnée et les finalités assignées au traitement.

19. Sur le plan qualitatif ensuite, la jurisprudence a précisé que seules les données factuelles et objectives peuvent en principe faire l'objet d'un traitement (CE, 11 mars 2013, n° 332886 ; Cons. Const. 15 novembre 2007, décision n° 2007-557 DC, loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile, cons. 29), ce qui revient à exclure la collecte de données subjectives fondées sur le « ressenti d'appartenance ».

Sous cet angle donc, la collecte des données relatives aux opinions ou aux croyances par définition subjectives doit en principe être écartée, à la différence des données relatives aux seules activités politiques, philosophiques, syndicales ou religieuses qui traduisent pour leur part un élément de fait objectif.

Le Conseil d'Etat a ainsi admis que le traitement de prévention des atteintes à la sécurité publique, lequel avait vocation à collecter des données concernant des personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives, puisse procéder à l'enregistrement des données relatives aux activités politiques, philosophiques, syndicales ou religieuses dès lors que les données collectées étaient exclusivement factuelles et objectives (CE, 11 mars 2013, n° 332886).

Sans doute, par exception à ce principe, le Conseil d'Etat a admis la collecte de données se rapportant à des opinions politiques, philosophiques, religieuses ou syndicales. Mais c'est dans l'unique mesure où, pour emprunter les termes de madame Bretonneau, « *il faut admettre, pour juger cette dérogation proportionnée, qu'une connaissance de certaines convictions politiques, philosophiques ou religieuses est pertinente pour évaluer la dangerosité d'un individu* » (A. BRETONNEAU, concl. lues sous : CE, 11 juillet 2018, Ligue des droits de l'homme, n° 414827).

Le traitement de données afférentes à des opinions politiques, philosophiques, religieuses ou syndicales a ainsi été admis pour le fichier ACCReD que dans la mesure où d'une part, ce traitement excluait la collecte de données relatives aux origines des personnes et, d'autre part, que seules étaient collectées les données indispensables à l'appréciation de la compatibilité du comportement des personnes lorsqu'il est de nature à porter atteinte à la sécurité publique avec l'exercice des fonctions ou des missions envisagées ou de l'atteinte que ce comportement pourrait porter à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'Etat (CE, 11 juillet 2018, *Ligue des droits de l'homme*, n° 414827).

Les données sensibles et à dimension subjective car relatives aux opinions politiques, philosophiques, religieuses ne peuvent en conséquence faire l'objet d'un traitement que de manière exceptionnelle, au regard d'une exigence d'adéquation et de pertinence renforcée, qui suppose que ces données soient indispensables pour que le traitement puisse répondre à sa finalité.

Il faut donc que le fichier ne donne lieu au traitement que de données adéquates et pertinentes qui, au regard de leur nature, reposent sur un périmètre limité et sur une appréciation factuelle et objective. Le respect de cette exigence est déterminant pour apprécier la proportionnalité de l'ingérence portée au droit au respect de la vie privée.

20. Il faut rappeler que le traitement litigieux avait uniquement vocation, en application R 236-2 du code de la sécurité intérieure, à collecter les données relatives aux motifs de l'enquête, les informations relatives aux coordonnées et à l'état civil, les photographies, les titres d'identité de l'intéressé ainsi que le rapport de l'enquête administrative, contenant les éléments permettant de déterminer si le comportement de la personne concernée n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées, compte tenu de leur nature.

De manière plus déroutante, l'article R. 232-3 ajoutait :

> « *L'interdiction prévue au I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique au traitement mentionné à l'article R. 236-1.*
> *Toutefois, l'enregistrement de données, contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des fonctions ou des missions envisagées est autorisé alors même que ce comportement aurait une motivation politique, religieuse, philosophique ou syndicale* » (soulignement ajouté).

L'article 2 du décret attaqué ajoute la collecte des données relatives :

- aux identifiants utilisés sur les sites internet et réseaux sociaux
- aux activités publiques ou au sein de groupements ou de personnes morales
- aux comportement et habitudes de vie
- aux déplacements
- aux activités sur les réseaux sociaux
- aux pratiques sportives
- aux pratiques et comportements religieux
- aux liens avec des groupes extrémistes
- aux éléments ou signes de radicalisation, suivi pour radicalisation
- aux données relatives aux troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur
- aux armes et titres afférents
- à la détention d'animaux dangereux

- aux antécédents judiciaires (nature des faits et date)
- aux fiches de recherche
- aux suites judiciaires
- aux mesures d'incarcération (lieu, durée et modalités)
- à l'accès à des zones ou des informations sensibles
- aux facteurs familiaux, sociaux et économiques
- aux régimes de protection
- aux faits dont la personne a été victime
- au comportement auto-agressif
- aux addictions
- aux mesures administratives ou judiciaires restrictives de droits, décidées ou proposées.
- à l'accès à des zones ou informations sensibles
- à l'indication de l'enregistrement de la personne dans six traitements de données à caractère personnel.

Enfin, l'article 3 modifie l'article R. 236-3 précité, de sorte que son deuxième alinéa dispose désormais que :

> « *Toutefois, l'enregistrement de données, contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des fonctions ou des missions envisagées est autorisé alors même que ce comportement aurait une motivation politique, religieuse, philosophique ou syndicale ou qu'il tiendrait à la dangerosité que feraient apparaitre les données, obtenues conformément aux dispositions législatives et réglementaires en vigueur, relatives aux troubles psychologiques ou psychiatriques de l'intéressé* » (soulignement ajouté).

De manière générale, ces données ne sont pas adéquates (i), le périmètre des individus concernés par la collecte est manifestement excessif (ii), et leur collecte n'est manifestement pas pertinente (iii).

(i) Sur le caractère inadéquat des données au regard de la nature des catégories de données susceptibles d'être collectées

21. De manière générale, la rédaction des différents items et des catégories de données susceptibles d'être collectées en application du décret attaqué est, ainsi que l'a d'ailleurs relevé la CNIL, particulièrement large et imprécise. Bien que la CNIL avait invité le Premier ministre à préciser le décret afin de délimiter de manière plus fine ce que recoupent ces catégories, elle n'a pas été entendue.

C’est ainsi que le décret vise des catégories d’informations en recours à des dénominations large et imprécises.

L’article 2 du décret autorise ainsi la collecte :

- «*des activités publiques ou au sein de groupements ou de personnes morales*» sans qualifier ces activités et groupements ni leur nature, ni préciser lesquelles des activités non publiques sont concernées,
- «*les comportements et habitudes de vie*» sans plus de précision,
- «*les déplacements*» sans que le décret ne précise s’il s’agit des déplacements à l’étranger ou des déplacements hors ou en métropole,
- «*les activités sur les réseaux sociaux*», sans que le décret ne précise les réseaux sociaux concernés ou indique la nature des activités visées telles que, par exemple, celles appelant à la haine ou à la violence,
- «*les pratiques sportives*», sans plus de précision,
- «*aux facteurs familiaux, sociaux et économiques*», sans plus de précision.

L’article 3 du décret autorise ensuite la collecte des données contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des fonctions ou des missions envisagées lorsque ce comportement « *tiendrait à la dangerosité que feraient apparaitre les données, obtenues conformément aux dispositions législatives et réglementaires en vigueur, relatives aux troubles psychologiques ou psychiatriques de l'intéressé* ».

Déjà sous cet angle, les données collectées sont, du fait de leur imprécision et de leur caractère stéréotypé, inadéquates.

Mais ce n’est pas tout.

22. S’agissant plus précisément de certaines de ces catégories de données, et en particulier des données relatives aux opinions politiques et aux convictions philosophiques, religieuses et syndicales, des données de santé, des données relatives aux activités sur les réseaux sociaux, ainsi que des données relatives aux antécédents et suites judiciaires, l’inadéquation est indéniable en raison des éléments suivants.

- **En premier lieu**, s'agissant des données relatives aux opinions politiques, aux convictions syndicales, religieuses et syndicales, l'article R. 236-3 autorise la collecte de données d'une extrême sensibilité qui, du fait de leur nature subjective, ne répondent pas à l'exigence d'adéquation.

  Ces dispositions n'autorisent pas simplement la collecte de données relatives aux activités politiques, philosophiques, religieuses, mais bien celles relatives aux opinions ou aux convictions qui impliquent un simple sentiment d'appartenance supposé à une communauté, comme les convictions présupposées des personnes, lesquelles sont par principe des données subjectives, et qui pour cette raison voient leur collecte en principe prohibée.

  Si le Conseil d'Etat a pu admettre la collecte de ce type de données c'est, on l'a vu, dans la seule mesure où certaines convictions sont susceptibles d'être pertinentes pour évaluer la dangerosité d'un individu. De la sorte, il est parfaitement illicite, et au mieux inutile, de collecter des données relatives aux opinions qui ne sont pas de nature à révéler un quelconque risque pour la société.

  On ne voit pas en effet en quoi une opinion qui n'est assortie d'aucun agissement répréhensible révélerait une quelconque dangerosité car l'émission d'une opinion, c'est-à-dire une pensée ou une réflexion qui n'est que le résultat de l'action de penser ou d'avoir un avis est en soi inoffensif.

  En toute hypothèse, l'appartenance à un syndicat, qui plus est un syndicat représentatif ne peut en aucun cas constituer une information révélatrice d'une menace, à elle-seule comme en articulation avec une autre information. Elle n'a aucune place dans un fichier dont la finalité est la prévention de menaces à la sécurité publique ou à la sûreté de l'Etat, et plus encore dans un fichier destiné à faciliter la réalisation d'enquêtes administratives.

  L'absence d'encadrement de la collecte de données subjectives extrêmement sensibles génère un risque inhérent de discrimination.

- **En deuxième lieu**, s'agissant des « addictions » ou « du comportement auto-agressif » visés par l'article 2 du décret, ainsi que des « *troubles psychologiques ou psychiatriques connus ou signalés* » auxquels renvoie l'article 3 du décret :

  La CNIL relevait à ce sujet dans son avis motivé sur ce décret que « *la Commission prend acte que les informations ainsi pourront être issues des traitements « prévention des atteintes à la sécurité publique » (PASP)* » (délibération n° 2020-066 du 25 juin 2020). Pourtant, la réglementation relative au traitement PASP ne renvoie à aucune disposition de cet ordre.

Il doit être rappelé que le secret médical consacré par l'article L. 1110-4 du code de la santé publique protège le droit au respect de la vie privée et le droit au secret des informations concernant toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le code de la santé publique.

Ce secret couvre, selon les mêmes dispositions, « *l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes, et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* » et s'impose « *à tous les professionnels intervenant dans le système de santé* », de sorte que la seule circonstance que l'information ne soit pas livrée par un professionnel de santé ne suffit pas à lever le secret médical (v. par exemple : CE, 25 novembre 2020, *conseil national de l'ordre des médecins*, n° 428451, mentionné aux tables).

Aussi, dès lors que ces données sont collectées par l'intermédiaire d'un professionnel de santé, d'un membre du personnel d'un établissement de santé, ou des membres d'un établissement, d'un service et d'un organisme qui, du fait de ses activités, est de près ou de loin en relation avec le système de santé, leur collecte et leur enregistrement méconnaît le secret médical.

Inversement, à supposer que la loi le permette, ne peuvent à l'évidence pas être collectées des données relatives à l'état de santé d'un individu qui ne proviendraient pas d'un professionnel de santé ou d'un établissement, service ou d'un organisme qui, du fait de ses activités, est en relation avec le système de santé. Nul ne peut en effet se prononcer sur la dangerosité d'un individu, ni sur ses troubles psychiatriques ou psychologiques en dehors d'un professionnel du monde médical, social ou médico-social.

Admettre le contraire reviendrait ni plus ni moins à rendre possible l'alimentation d'un traitement automatisé par des informations recueillies auprès des proches ou des contacts de l'intéressé, subjectives ou erronées, dont la fiabilité ne pourra pas être vérifiée, sans aucune garantie d'objectivité.

On ne comprend ni l'étendue du fichage ni les modalités selon lesquelles ces informations seront collectées, et on ne voit pas les garanties pour les intéressés quant à la licéité de cette collecte et quant à la crédibilité des informations en cause.

- **En troisième lieu**, s'agissant des données relatives aux «*identifiants utilisés sur les réseaux sociaux* » ou aux « *activités sur les réseaux sociaux* » :

  D'abord, la rédaction du décret indique que l'activité des individus sur l'ensemble des réseaux sociaux est concernée par la collecte y compris les données introduites sur des pages qui ne sont pas en sources ouvertes enregistrées sur des pages ou des comptes protégés par un mot de passe, ce qui reviendrait ni plus ni moins à autoriser un « *piratage* » des comptes des citoyens.

  Ensuite, le décret ne dit rien des données collectées qui mettent en cause des tiers. L'activité sur les réseaux sociaux suppose par définition des interactions avec les tiers, qu'il s'agisse d'une adhésion à une publication d'un tiers, du partage d'une publication d'un tiers, ou d'un dialogue avec un tiers, de sorte qu'on voit mal comment des données relatives à l'activité d'un individu sur les réseaux sociaux pourraient être collectées abstraction faite des données qui concernent des tiers.

  Enfin, rien n'est dit des activités et des données susceptibles d'être concernées par la collecte et les dispositions attaquées ne limitent pas la collecte aux seules activités qui conduiraient à appeler à la haine ou à la violence. On ignore les réseaux sociaux concernés, le type de revendication ou de publication qui pourront justifier un enregistrement de données, et enfin les dispositions attaquées n'excluent pas, et par conséquent, ouvrent la possibilité d'une collecte automatisée de ces données.

  Dès lors qu'il vise les identifiants et les activités sur les réseaux sociaux, c'est une surveillance généralisée de n'importe quelle activité sur n'importe quel réseau social qui est prévue et qui donne lieu à une collecte de données.

- **En quatrième et dernier lieu,** s'agissant des données relatives aux « *antécédents judiciaires* », aux « *suites judiciaires* » et « aux mesures administratives ou judiciaires restrictives de droits, décidées ou proposées », leur collecte méconnaît les dispositions de l'article 777-3 du code de procédure pénale.

  Suivant cet article, « *aucun fichier ou traitement de données à caractère personnel détenu par une personne quelconque ou par un service de l'Etat ne dépendant pas du ministère de la justice ne pourra mentionner, hors les cas et dans les conditions prévus par la loi, des jugements ou arrêts de condamnation* ».

Les dispositions critiquées autorisent en conséquence la collecte de données relatives aux antécédents judiciaires et aux décisions juridictionnelles prises à leur encontre, telles que les jugements ou arrêts de condamnation. D'ailleurs, la CNIL rappelait dans son avis «*que la collecte de données relatives aux catégories précitées ne pourra en aucun cas porter sur des jugements ou des arrêts de condamnations, conformément aux dispositions de l'article 777-3 du code de procédure pénale*» (délibération n° 2020-065 du 25 juin 2020).

Force est cependant de constater que le décret persiste à mentionner les « antécédents judiciaires », « suites judiciaires » et « mesures administratives ou judiciaires restrictives de droits, décidées ou proposées » sans autre précision, ce qui ne garantit pas que le traitement litigieux respecte l'exigence fixée par l'article 777-3 du code de procédure pénale en excluant toute mention des condamnations pénales.

Ce défaut d'adéquation est aggravé par l'extrême sensibilité des données et par l'indétermination du cadre juridique dans lequel elles peuvent être collectées.

A l'absence de pertinence déjà constatée et à l'inadéquation ainsi établie pour un grand nombre de données, s'ajoute encore la circonstance que l'étendue des individus dont les données sont susceptibles d'être collectées est manifestement excessive.

(ii) Sur le périmètre excessif des données collectées en raison de l'étendue des personnes concernées par la collecte

23. On l'a vu, le traitement « EASP» est un fichier rempli et consulté lorsqu'un individu fait l'objet « *d'enquêtes administratives en application des articles L. 114-1, L. 114-2 et L. 211-11-1 du présent code et de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité*».

Ce sont donc l'ensemble des personnes faisant l'objet ou ayant fait l'objet d'une enquête administrative en application de ces dispositions qui sont concernées par la collecte de données dans le traitement litigieux, si bien qu'à la différence de la majorité des autres fichiers, le fichier « EASP » ne concerne pas les seules personnes dont le comportement ou les activités seraient susceptibles de constituer une menace.

En application de l'article L. 114-1 du code de la sécurité intérieure sont ainsi concernées :

- tout agent public qui participe ou qui souhaite participer à l'exercice des missions de souveraineté de l'Etat,
- tout agent public ou salarié qui occupe ou qui souhaite occuper un emploi relevant du domaine de la sécurité ou de la défense,
- tout salarié ou non salarié qui occupe ou qui souhaite occuper un emploi ou une activité réglementée relevant du domaine des jeux, paris et courses,
- toute personne qui souhaite accéder à une zone protégée en raison de l'activité qui s'y exerce
- toute personne qui souhaite utiliser des matériels ou produits présentant un caractère dangereux.

En application de l'article L. 114-2 du code de la sécurité intérieure sont concernées :

- toute personne qui occupe ou qui souhaite occuper un emploi en lien avec la sécurité des personnes et des biens au sein d'une entreprise publique de transport de personnes,
- toute personne qui occupe ou qui souhaite occuper un emploi en lien avec la sécurité des personnes et des biens au sein d'une entreprise de transport de marchandises dangereuses.

En application de l'article L. 211-11-1 du code de la sécurité intérieure est concernée :

- toute personne autre qu'un participant ou un organisateur souhaitant accéder à des établissements ou des installations qui accueillent des grands évènements.

En application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité sont concernés :

- tout étranger en situation régulière ou irrégulière qui entend prétendre à un titre de séjour
- tout étranger souhaitant acquérir la nationalité française
- tout étranger titulaire d'un titre de séjour.

En définitive, tout citoyen français, toute personne résidente en France et toute personne souhaitant y résider est susceptible de voir ses données

personnelles collectées dans ce fichier, et ceci indépendamment de leur comportement ou de la menace qu'elle serait susceptible de créer.

Et il faut ajouter à cela que le traitement ne se limite pas à collecter et enregistrer les données des personnes majeures mais s'étend également aux personnes mineures de plus de seize ans.

Dans ces conditions, faute de porter sur un nombre restreint d'individus, le champ des personnes susceptibles de voir leurs données collectées dans ce traitement est manifestement trop large.

(iii) Sur l'absence de pertinence des données au regard de la finalité censée justifier la collecte et le traitement

24. L'absence de pertinence des données trouve sa cause dans le fait que le décret n'introduit aucune distinction au sein des données susceptibles d'être collectées en fonction de la nature et de la sensibilité de l'enquête administrative.

On l'a vu, les enquêtes administratives visées à l'article R. 236-1 du code de la sécurité intérieure soumettent l'adoption de décisions administratives nombreuses, très diverses et ne présentant pas toutes le même degré de sensibilité.

Compte tenu de la diversité des données susceptibles d'être collectées, la CNIL reprochait au décret de ne pas introduire de distinction au sein des données collectées :

> *« En revanche, la Commission estime que les dispositions projetées ne permettent pas de rattacher de manière exclusive les données concernées à la finalité pour laquelle elles sont traitées. Dès lors, ces dispositions ne permettent pas aux personnes concernées de déterminer avec certitude les modalités selon lesquelles elles peuvent exercer leurs droits. (…)*
> *La Commission considère que la mise en œuvre de marqueurs spécifiques, ou d'un dispositif équivalent, doit permettre de déterminer précisément les données considérées comme intéressant la sûreté de l'Etat, sur la base de critères précis. Une telle identification est de nature à permettre au responsable de traitement saisi d'une demande d'exercice des droits sur le fondement du titre III de la loi du 6 janvier 1978 modifiée*

> *de n'exclure de sa réponse que les données identifiées par avance, et sur la base de critères précis, comme relevant du régime du titre IV. (…)*
> *Dès lors qu'il s'agit d'une modalité essentielle de l'exercice des droits en présence d'un fichier relevant à la fois du titre III et du titre IV de la loi, la Commission estime que le décret devrait préciser que les données relevant du titre IV sont identifiées comme telle dans le fichier. En tout état de cause, elle considère qu'en l'absence de dispositions ou de mesures permettant une identification objective des données exclues du droit d'accès direct, l'application des dispositions du titre III de la loi du 6 janvier 1978 modifiée devrait prévaloir.»* (délibération n° 2020-066 du 25 juin 2020).

Force est cependant de constater que la CNIL n'a pas été entendue et que le décret s'abstient de préciser la nature des données susceptible d'être collectées suivant le type d'enquête administrative mise en œuvre, de sorte qu'on peut redouter que les données collectées dans le cadre de n'importe quelle enquête administrative nourrisse finalement le renseignement pour la sûreté de l'Etat.

Pour le dire autrement, faute de préciser que certaines de ces données ne peuvent être collectées et enregistrées que lorsque la réalisation de l'enquête administrative consiste à s'assurer que l'individu ne présente pas de menace pour la sûreté de l'Etat. Le décret permet, quelle que soit l'enquête administrative réalisée, la collecte de données personnelles parmi lesquelles certaines sont d'une sensibilité accrue.

Or, la collecte des données relatives à une enquête administrative s'apprécie exclusivement au regard de l'objet de la décision administrative qui sera prise à son issue et n'a pas nécessairement pour finalité de protéger la sûreté de l'Etat.

Sous couvert de sûreté de l'Etat, le décret litigieux permet de rassembler des informations très sensibles – relatives aux troubles psychologiques ou psychiatriques, aux opinions politiques, aux convictions philosophiques, religieuses ou syndicales, aux addictions ou aux activités sur les réseaux sociaux– alors même que ces personnes ne présentent aucune menace, que l'enquête administrative réalisée est dépourvue de tout lien avec la sûreté de l'Etat, et que les données ne se rapporte à aucune menace.

Rien ne justifie pourtant que soient collectées, enregistrées et traitées les données relatives, par exemple, à l'activité d'un individu sur les réseaux sociaux, à son appartenance religieuse, ou à ses activités au sein de syndicats ou d'association au motif qu'il fait l'objet d'une enquête

administrative parce qu'il souhaite exercer l'emploi de buraliste ou acquérir la nationalité française.

Il s'agit là d'une pure logique de maximisation des informations qui consiste à rassembler des informations dont certaines sont sans lien préétabli avec la finalité poursuivie.

25. A cela s'ajoute la circonstance que les règles de mise en œuvre du traitement ne distinguent pas au sein des données susceptibles d'être collectées celles dont la collecte est justifiée par la sensibilité de l'enquête administrative réalisée .

Concrètement, les données relatives à l'état civil de l'intéressé, à son appartenance religieuse, ou à ses activités sur les réseaux sociaux pourront être collectées de la même façon pour un individu qui sollicite un titre de séjour, une autorisation pour ouvrir un bureau de tabac ou l'autorisation de disposer d'un port d'armes.

Ensuite, s'agissant du traitement des données ainsi collectées, il soumet à un seul et unique régime les données des personnes susceptibles d'être collectées à l'occasion d'une simple enquête administrative, par exemple pour l'octroi d'un titre de séjour, et celles qui celles qui sont susceptibles de se rattacher à la sûreté de l'Etat parce qu'elles portent, par exemple, sur l'accès à une zone protégée en raison de l'activité qui y est exercée.

A titre d'illustration, et ainsi qu'il sera vu, ces données peuvent être conservées pour une même durée de cinq ans indépendamment de la finalité motivant leur enregistrement, et le décret ne distingue pas plus les destinataires de ces données en raison de la nature des données collectées ou du type d'enquête administrative réalisée.

Cette confusion entre la sensibilité des données traitées et la diversité des enquêtes administratives à l'occasion desquelles ces données sont collectées revient à priver les personnes concernées de garanties dès lors qu'on l'a vu, les traitements automatisés qui intéressent la sûreté nationale et la défense nationale ne sont pas soumis au droit de l'Union mais aux seules dispositions spécifiques de la loi n°78-17 du 6 janvier 1978 qui posent des garanties moindres.

Il eut été possible de moduler l'étendue des données enregistrées selon les finalités des enquêtes administratives à l'occasion desquelles les données sont collectées.

Compte tenu de ce que les données sont collectées indifféremment de la sensibilité de l'enquête administrative menée, le critère de la pertinence des données collectées n'est pas satisfait.

26. Partant, en tant qu'il autorise la collecte de données qui ne sont ni adéquates, ni pertinentes et qui excèdent ce qui est nécessaire pour la mise en œuvre de ses finalités, le décret porte au droit au respect de la vie privée et à la liberté d'opinion, de conscience et de religion une atteinte qui est d'ores et déjà excessive.

Mais ce n'est pas tout, s'ajoute à cela le périmètre excessivement étendue de l'accès au traitement ainsi que le caractère excessif de la durée de conservation des données.

B.1.3. Sur le périmètre excessivement étendu de l'accès aux données

27. L'étendue du périmètre des destinataires et sa pertinence s'apprécient au regard de sa précision, du nombre de destinataires, de leur qualité, de la nature et de l'ampleur des données en cause, et enfin des restrictions posées pour l'accès aux données (CE, 24 avril 2019, n° 419498, mentionné aux tables).

L'accès aux données doit être réservé aux personnes qui exercent une mission en lien avec les finalités poursuivies et, en cas d'accès par une personne morale ou un organisme, à des personnes en charge de mettre en œuvre ces missions, à défaut de quoi les dispositions concernées sont censurées (CE, 21 septembre 2015, *ADAJIS*, n°389815 ; v. également : Cons. Const. 11 mai 2020, décision 2020-800, loi prorogeant l'état d'urgence sanitaire, cons. 70).

Outre sa nécessité, le périmètre des destinataires doit être suffisamment précis, limité et restreint, étant entendu que l'accès aux données

peut également être régulé par l'institution d'un droit d'accès indirect soumis à une demande motivée répondant à des conditions prédéfinies.

A cet égard, le Conseil d'Etat a retenu, pour admettre la légalité d'un traitement que les personnes ayant directement accès aux données étaient limitativement et spécialement énumérées et que si tout autre agent de police ou de gendarmerie pouvait accéder aux données, ce n'était que de manière indirecte à la suite d'une demande expresse précisant son identité, l'objet et les motifs de sa demande, celle-ci devant être agréée par les responsables des services ayant habituellement accès au traitement (CE, 11 mars 2013, n° 332886 ; v. également dans le même sens : CE, 30 décembre 2009, association SOS Racisme, n° 312051, publié au Lebon).

Inversement, le fichier porte au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi lorsqu'un grand nombre de personnes est susceptible d'accéder fréquemment à un traitement ample, ceci en l'absence de garanties suffisantes (Cons. Const., 13 mars 2014, décision n° 2014-690 DC, loi relative à la consommation, cons. 57).

Il faut ajouter à cela que la limitation des personnes susceptibles d'avoir un accès aux données et le souci de confidentialité des données est encore justifié par l'exigence d'efficacité des outils de renseignement et, à cet égard, l'accès des élus locaux à ce type de fichier est largement discuté voire critiqué (rapport d'information n°1335 sur les fichiers mis à disposition des forces de sécurité enregistré le 17 octobre 2018, page 52).

28. Dans le cas présent, dans sa rédaction issue du décret attaqué, l'article R. 236-6 du code de la sécurité intérieure distingue les personnes qui peuvent accéder au fichier et ainsi connaître l'ensemble des données qui y sont enregistrées, des personnes qui peuvent être destinataires de données contenues dans le fichier.

S'agissant d'abord des personnes pouvant accéder au fichier, l'article R. 236-6 prévoit :

> « *I. – Dans la limite du besoin d'en connaître, en vue de la réalisation d'enquêtes administratives, sont autorisés à accéder aux données mentionnées aux articles R. 236-2 et R. 236-3 :*
> *1° Les agents relevant du service central du renseignement territorial de la direction centrale de la sécurité publique,*

individuellement désignés et spécialement habilités par le directeur central de la sécurité publique ;
2° Les agents affectés dans les services du renseignement territorial des directions départementales de la sécurité publique ou des directions territoriales de la police nationale, individuellement désignés et spécialement habilités par le directeur départemental ou par le directeur territorial ;
3° Les agents affectés dans les services de la préfecture de police chargés du renseignement, individuellement désignés et spécialement habilités par le préfet de police ».

S'agissant ensuite des personnes qui peuvent être destinataires de données contenues dans le fichier, l'article R. 236-6 prévoit :

« *II. – Dans la limite du besoin d'en connaître, en vue de la réalisation d'enquêtes administratives, peuvent être destinataires des données mentionnées aux articles R. 236-2 et R. 236-3 :*
1° 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 ;
2° 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 ;
3° Tout autre agent d'une unité de la gendarmerie nationale ou d'un service de la police nationale, sur demande expresse précisant l'identité du demandeur, l'objet et les motifs de la consultation. Les demandes sont agréées par les responsables des services mentionnés aux 1°, 2° ou 3° du I.».

29. D'ores et déjà, ainsi que le démontre le dernier item, ces dispositions permettent l'accès à ces données d'une extrême sensibilité aux forces de l'ordre alors même qu'elles ne seraient dotées d'aucune mission de renseignement.

Ce sont ainsi 150.000 agents de la police nationale et 102.000 agents de la gendarmerie nationale qui peuvent accéder aux données personnelles enregistrées dans ce traitement et dont on a vu qu'elles peuvent concerner toute personne faisant ou ayant l'objet d'une enquête administrative.

La circonstance que ces derniers doivent demander à consulter les informations pour y accéder ne constitue pas de toute évidence une garantie suffisante pour les raisons suivantes :

D'abord, la seule limite posée par ces dispositions est « *le besoin d'en connaître* », ce qui est imprécis, sans limite de l'étendue des destinataires au regard de la finalité poursuivie.

Ensuite, les dispositions attaquées ne précisent pas les données qui peuvent être effectivement transmises, si bien que sur simple demande il peut légitimement être craint que l'agent de police accède à l'intégralité de la fiche de toute personne enregistrée dans le traitement et ainsi à l'ensemble des données relatives à l'individu concerné y compris celles qui ne seraient pas pertinentes au regard de l'objet de la demande.

Enfin, faute de critère précis, le responsable du traitement à qui les informations sont demandées n'est assurément pas en mesure de s'assurer que la transmission des données est justifiée à raison des attributions du demandeur ou des limites de sa compétence. Il n'existe en outre aucun contrôle des motifs présentés à l'appui de la demande d'informations.

Compte tenu de la sensibilité des données et du nombre de personnes concernées, il est impossible de se satisfaire de la seule garantie prise de ce que la demande émane de personnels de la police nationale ou de militaires de la gendarmerie nationale.

Mais ce n'est pas tout.

30. En tant qu'il renvoie largement au terme « d'enquêtes administratives », le décret permet à l'intéresser d'accéder aux données enregistrées pour n'importe quelle enquête et même si l'objet de l'enquête ne nécessite pas d'avoir accès à des informations semblables à celles qui concernent les opinions et convictions politiques, philosophiques, syndicales religieuses, ou aux données de santé révélant des troubles psychologiques ou psychiatriques.

31. Enfin, le fichier « EASP » est interconnecté avec un autre fichier : le fichier dénommé «Automatisation de la consultation centralisée de

renseignements et de données » (ACCReD) qui a également pour finalité de faciliter la réalisation d'enquêtes administratives.

De cette interconnexion résulte la possibilité pour les personnes disposant d'un accès à ACCReD d'identifier si les données de la personne visée sont enregistrées dans le fichier « EASP » recueillies pour une personne visée. L'article 7 du décret n° 2017-1224 du 3 août 2017 dispose à cet égard que :

> « *I. - Le traitement mentionné à l'article 1er peut procéder à la consultation automatique et, le cas échéant, simultanée des traitements de données à caractère personnel suivants aux seules fins de vérifier si l'identité de la personne concernée y est enregistrée :*
> *(...)*
> *2° Le traitement automatisé de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » mentionné aux articles R. 236-1 et suivants du code de la sécurité intérieure ;* ».

Ceci permet un accès indirect, puisque l'agent qui peut consulter une fiche dans le traitement ACCRed peut demander à un agent visé par les dispositions du I ou du II de l'article R. 232-6 précité, de lui communiquer l'information, ce que l'intéressé pourra faire dès lors qu'il estime que cette consultation peut être utile pour l'enquête administrative.

Or, sont notamment autorisées à accéder à ce fichier ou à des données de ce fichier, en application de l'article 5 du décret précité du 3 août 2017 : les agents d'un service du ministère de l'intérieur chargé d'effectuer une enquête administrative visée à l'article 1er de l'article R. 236-1 précité, les personnes morales ou l'autorité administratives pour les données relatives au résultat de l'enquête ainsi que le préfet du département concerné.

Le caractère excessif du périmètre des destinataires de ces données est ainsi aggravé par l'interconnexion entre les deux fichiers.

Le décret met ainsi en place un accès au fichier dont le périmètre est exclusivement étendu sans aucune garantie quant aux conditions auxquelles est soumis cet accès.

B.1.4. Sur le caractère excessif de la durée de conservation des données

32. Le 5° de l'article 4 précité de la loi n°78-17 du 6 janvier 1978 prévoit que la durée de conservation des données collectées ne doit pas excéder le temps nécessaire à la poursuite de la finalité (v. également : CE, 30 décembre 2009, *association SOS Racisme*, n° 312051, publié au Lebon ; CE, 19 juillet 2010, n°334014, mentionné aux tables ; CE, 11 juillet 2018, n° 414827).

La proportionnalité de la durée de conservation des données doit également être appréciée à la lumière des données collectées et, sur ce point, la Cour européenne des droits de l'homme indique que les données révélant les opinions notamment politiques des individus doivent faire l'objet d'une protection accrue, si bien que leur conservation prolongée porte une atteinte disproportionnée au droit au respect de la vie privée (CEDH, 24 janvier 2019, *Catt. c. Royaume-Unis*, 43514/15, §112).

33. La durée de conservation des données doit également être appréciée globalement lorsque le traitement fait l'objet d'une interconnexion, d'un rapprochement, ou d'une quelconque autre forme de mise en relation. De manière générale, la simple mise en relation suppose toute « *mise en relation systématique de deux fichiers n'ayant pas pour effet d'élargir le périmètre de collecte d'aucun des deux* » (A. BRETONNEAU, concl. lues sous : CE, 21 septembre 2015, n° 390070).

Ce terme générique recouvre plusieurs réalités distinctes que sont l'interconnexion – c'est-à-dire le branchement informatisé de deux fichiers dont le périmètre ne se recouvre pas (CE, 19 juillet 2010, n° 317182) –, et le rapprochement, lequel peut être caractérisé par la simple consultation simultanée de deux fichiers distincts.

Lorsqu'un fichier a vocation à alimenter un second fichier, la durée de conservation des données collectées doit être examinée au regard de la durée de conservation des données traitées par le second fichier. En effet, lorsqu'elles sont transférées dans un second fichier, les données ont désormais vocation à être conservée pendant la durée maximale de conservation prévue par ce second fichier, de sorte que la durée de conservation des données telle qu'elle est prévue par le second fichier dans lequel les données collectées sont transférées se substitue à celle prévue par le fichier initial.

34. Dans le cas présent, l'article R. 236-4 du code de la sécurité intérieure prévoit que les données collectées peuvent être conservées pendant une durée de cinq ans à compter de leur enregistrement, sans distinction de ce que la personne est mineure ou majeure.

Concrètement, un individu dont les données sont collectées par ce qu'il sollicite une autorisation pour l'ouverture d'un débit de boisson ou pour se voir octroyer un port d'arme verra ses données conservées de la même manière pendant cinq années.

Pour l'ensemble de ces motifs, la durée de conservation des données n'est pas fixée de manière proportionnée.

35. Il faut ajouter à cela que le décret attaqué indique la mention de la personne intéressée dans d'autres traitements.

L'article 5 du décret attaqué prévoit à cet égard que :

> « *Art. R. 236-7.-Les opérations de collecte, de modification, de consultation, de communication, de transfert, de rapprochement et de suppression des données à caractère personnel et informations font l'objet d'un enregistrement comprenant l'identifiant de l'auteur, la date, l'heure et le motif de l'opération et, le cas échéant, les destinataires des données. Ces informations sont conservées pendant un délai de trois ans.»* (soulignement ajouté)

Le décret prévoit ainsi la possibilité de rapprocher le « EASP » d'autres fichiers et ajoute aux dispositions existantes, lesquelles ne prévoyaient pas jusqu'alors la possibilité d'un quelconque rapprochement.

Par ailleurs, l'article 2 du décret ajoute au sein des catégories de données collectées la mention de l'enregistrement de la personne concernée dans un autre traitement, ce qui implique l'enregistrement d'informations résultant de l'interrogation ou de la consultation des fichiers suivants :

- le traitement d'antécédents judiciaires (TAJ) ;
- le système informatique national N-SIS II ;

- le traitement automatisé de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique » (PASP) ;
- le traitement automatisé de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP) ;
- le fichier des personnes recherchées (FPR);
- le traitement automatisé de données à caractère personnel dénommé « FSPRT » ;
- le traitement automatisé des données relatives aux objets et véhicules volés ou signalés (FOVeS).

Dans la mesure où le décret attaqué autorise un rapprochement entre le « EASP » et d'autres traitements de données, la durée de conservation des données enregistrées dans le « EASP » doit être appréciée à la lumière de la durée de conservation des données des autres traitements. Or, s'agissant par exemple du TAJ, les données sont conservées dans ce traitement pour une durée maximale de quarante ans en application de l'article R. 40-27-I du code de procédure pénale.

La durée de conservation des données collectées et traitées par le traitement « EASP » excède en conséquence ce qui est nécessaire pour la mise en œuvre de la finalité assignée au traitement.

B.1.5. Sur le caractère disproportionné de l'atteinte portée au droit au respect de la vie privée et à la liberté d'opinion, de conscience et de religion

36. Il résulte de tout ce qui précède qu'en raison de la seconde finalité qu'il assigne au décret et de la confusion qu'elle génère, le décret prive le fichier de sa finalité claire et légitime, outre qu'il autorise la collecte de données qui, de par leur nature, ne sont ni adéquates ni pertinentes au regard des finalités poursuivies.

Enfin, l'atteinte ainsi portée au respect de la vie privée et à la liberté d'opinion, de conscience et de religion est encore aggravée par le caractère excessif de l'accès aux données et de leur durée de conservation.

En raison de l'ensemble de ces éléments, le décret porte une atteinte disproportionnée au droit au respect de la vie privée et à la liberté d'opinion, de conscience et de religion.

L'annulation est inéluctable.

B.2.] Sur la violation de l'article 4 de la loi n°78-17 du 6 janvier 1978 à raison de l'absence de finalité claire et légitime donnée au traitement litigieux, du caractère inadéquat et non pertinent des données collectées, le périmètre excessivement étendu de l'accès aux données et de la durée excessive de conservation des données

37. Aux termes de l'article 4 de la loi n°78-17 du 6 janvier 1978 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. »

Ces dispositions posent une triple exigence puisqu'elles prévoient que les données doivent être adéquates et pertinentes au regard des finalités poursuivies (ii), qu'elles doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (iii) et qu'elles doivent être traitées de façon à garantir une sécurité appropriées en raison notamment de leur conditions d'accès (iv).

38. Or, il résulte de ce qui précède que :

- les données collectées ne sont ni adéquates ni pertinentes,
- la durée excède celle nécessaire au regard des finalités pour lesquelles elles sont traitées
- le périmètre de l'accès aux données est manifestement trop large.

Partant, prises isolément, chacune des exigences posées par l'article 4 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ici méconnue.

L'annulation est pour ce nouveau motif encourue.

B.3] <u>Sur la méconnaissance de l'article 88 de la loi n°78-17 du 6 janvier 1978, ensemble l'article 1er de la Constitution, le droit au respect de la vie privée et la liberté de pensée, de conscience et de religion en ce que le décret autorise la collecte de données relevant de l'article 6 de la loi du 6 janvier 1978 sans nécessité absolue et en l'absence de garantie appropriée</u>

39. Le droit applicable distingue au sein des données personnelles les données dites sensibles dont le traitement est en principe prohibé en application de l'article 6 de la loi du 6 janvier 1978 et qui sont relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, aux données biométriques ou génétiques, ou aux données concernant la santé, la vie sexuelle ou l'orientation des personnes physiques.

L'article 88 de la même loi applicable aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales prévoit que le traitement de ces données sensibles « *est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits libertés de la concernée* » et il appartient en conséquence au responsable du traitement de justifier des circonstances rendant ainsi indispensable le traitement des données les plus sensibles visées à l'article 6 de la loi du 6 janvier 1978.

40. Or, aucune des deux conditions cumulatives posées par ces dispositions pour le traitement de données sensibles n'est satisfaite par le décret.

B.3.1] Sur l'absence de définition des cas de nécessité absolue

41. Le décret attaqué ne soumet pas la collecte de ces données à une nécessité absolue, outre qu'il n'introduit aucune distinction entre la collecte des données sensibles et les autres, de sorte que les données relatives à l'état civil et celles relatives aux opinions politiques, philosophiques, syndicales ou religieuses ou les données de santé peuvent être collectées dans les mêmes conditions.

L'auteur du décret s'est ainsi abstenu d'encadrer les cas dans lesquels les agents peuvent s'estimer fondés à collecter ces données. L'appréciation de cette nécessité est ainsi laissée à la seule discrétion des agents concernés, et il ne peut être exclu que la collecte des informations soit privilégiée même en l'absence d'impérative nécessité « au cas où » ces données pourraient avoir vocation dans le futur à servir.

En s'abstenant de définir les cas dans lesquels la collecte de ces données est possible, le décret institue la possibilité de collecter toute donnée, indépendamment des nécessités, dans une pure logique de maximation des données.

B.3.2] Sur l'absence de garantie appropriée

42. D'autre part, on ne voit pas quelles sont les garanties auxquelles le décret a assorti la collecte de ces données sensibles, alors que leur extrême sensibilité imposait de plus fort de telles garanties.

Le décret ne prévoit même pas que ces données sont collectées dans la stricte mesure où elles seraient nécessaires à la poursuite des finalités définies par le décret.

Il s'ensuit que le fichier litigieux peut contenir toutes les informations relevant des catégories énoncées par le décret attaqué, y compris celles visant des données extrêmement sensibles, ceci sans aucune limite, et sans aucune garantie pour les citoyens.

43. Ainsi, faute de définir les cas de nécessité absolue et d'assortir la collecte des données personnelles dites « sensibles » de garanties, le décret méconnaît l'article 88 de la loi n° 78-17 du 6 janvier 1978 et l'article 1er de la Constitution, et porte une atteinte injustifiée au droit au respect de la vie privée et à la liberté d'opinion, de conscience et de religion.

A tous les égards, l'annulation s'impose.

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

- **ANNULER** le décret n° 2020-1510 du 2 décembre 2020

- **METTRE À LA CHARGE** de la charge de l'Etat le versement à chacun des requérants d'une somme de 1.000 euros en application de l'article L. 761-1 du code de justice administrative
  .

Pour la S.C.P. Anne SEVAUX et Paul MATHONNET,
l'un d'eux

Productions

1 décret n° 2020-1510 du 2 décembre 2020