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° 2020-1512 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique» (**GIPASP**) (**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).

Puis le décret n°2011-340 du 29 mars 2011 a institué le traitement dénommé «Gestion de l'information et prévention des atteintes à la sécurité publique» ou «GIPASP», qui se présente comme le pendant, pour la gendarmerie, du fichier de la police nationale «PAPS» précité. Ses dispositions ont été codifiées aux articles R.236-21 à R.23-30 du code de la sécurité intérieure.

2. Le GIPASP, de même d'ailleurs que le PASP dont le cadre juridique est identique, avait alors pour unique finalité « *de recueillir, de conserver et d'analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique* » et en particulier les informations qui concernent les *« personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives* » (soulignement ajouté).

Le système est alimenté, en premier lieu, par des fiches de renseignement simplifié (FRS) rédigées au niveau des « unités élémentaires », en particulier les brigades territoriales, pour rapporter des informations d'ordre public. Elles peuvent être créées et sont visibles de toute personne ayant un droit d'accès à GIPASP (soit initialement environ 84 000 agents).

Au niveau des groupements de gendarmerie départementale et des bureaux renseignements des régions de gendarmerie, les cadres du renseignement (chefs des bureaux renseignement, officiers adjoints renseignement (OAR) et analystes renseignement), au nombre de 2 300, exploitent les informations contenues dans les FRS et rédigent, s'il y a lieu, des fiches de renseignement élaboré (FRE) ou des fiches de renseignement élaboré confidentielles (FREC) ainsi que des fiches entité (FIE). Les FREC sont conservées, tout comme les FRE, dix ans.

Le «GIPASP» a connu une montée en puissance progressive et au 1er juillet 2017, 40 474 individus y étaient recensés.

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 PAPS en ajoutant à leur finalité initiale celle consistant à recenser les menaces susceptibles d'être portées à la sûreté de l'Etat. Par voie de conséquence, il les a fait relever pour partie du titre IV de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Il a également décidé de modifier les fichiers EASP, PAPS et GIPASP en élargissant les catégories de données susceptibles d'être collectées, ainsi que l'étendue des destinataires des données.

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 «GIPASP» a été soumis à la consultation préalable de la CNIL qui a émis à son sujet une délibération n° 2020-065 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° 2020-1512 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 «Gestion de l'information et prévention des atteintes à la sécurité publique» ou «GIPASP» (**production n°1**).

5. De manière générale, les modifications consistent à élargir les finalités du traitement qui visait initialement, on l'a vu, les seules personnes dont l'activité individuelle ou collective indiquant qu'elles puissent porter atteinte à la sécurité publique. Le décret du 2 décembre 2020 y ajoute que sont également visées les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sûreté de l'Etat.

Ainsi qu'il résulte de l'article 1er du décret, le traitement a ainsi désormais pour finalité de recueillir, de conserver et d'analyser les informations qui concernent :

- 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,
- les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives, au titre de la sécurité publique.

Le même article précise également que les personnes susceptibles d'être enregistrées dans le traitement peuvent être des personnes physiques, des personnes morales, ainsi que des groupements.

En somme, et ainsi que l'a relevé la CNIL dans sa délibération du 25 juin 2020, le traitement GIPASP tel qu'il a été modifié n'intéresse que pour partie la sûreté de l'Etat et vise à prévenir des atteintes de nature très diverses relevant en réalité bien plus de la sécurité publique.

Sans distinguer l'une ou l'autre des deux finalités, l'article 2 de ce décret autorise la collecte et l'enregistrement de nouvelles catégories de données telles que celles relatives aux activités sur les réseaux sociaux, aux comportements ou habitudes de vie, aux pratiques sportives, aux pratiques et comportements religieux, aux facteurs de dangerosité, aux données relatives aux troubles psychologiques ou psychiatriques, aux addictions aux facteurs familiaux, sociaux et économiques ou des addictions, aux antécédents judiciaires, et il prévoit l'ajout de la mention de l'enregistrement de la personne concernée dans un autre traitement.

Mais ce n'est pas tout, car l'article 3 ajoute, nonobstant l'interdiction prévue au I de l'article 6 de la n° 78-17 du 6 janvier 1978, là encore

sans distinguer selon la finalité poursuivie, que peuvent également être collectées les données relatives aux opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale ainsi que les données de santé révélant une dangerosité particulière.

L'article 2 du décret étend également la collecte de données aux personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec les personnes ou groupements pouvant porter atteinte à la sécurité publique ou la sûreté de l'Etat, ainsi qu'aux victimes des agissements de ces personnes ou groupements.

Le même article supprime enfin la mention jusqu'alors prévue à l'article R. 236-22 du code de sécurité intérieure qui prévoyait que le traitement ne comportait pas de dispositif de reconnaissance faciale à partir de la photographie.

L'article 6 étend la possibilité de consulter les données collectées aux personnes ayant autorité sur les agents du service national des enquêtes administratives de sécurité et sur les agents du commandement spécialisé pour la sécurité nucléaire, aux procureurs de la République, ainsi qu'aux agents de la police nationale ou d'une unité de gendarmerie nationale qu'ils soient ou non chargés d'une mission de renseignement sur autorisation expresse des commandants, et ceci quelle que soit la finalité poursuivie.

L'article 7 substitue au délai de cinq ans prévu pour la conservation des données relatives à la consultation du traitement un délai de trois ans, et enfin, l'article 8 précise que les droits des personnes s'exercent de manière différente selon que les données intéressent ou non la sûreté de l'Etat.

6. Le décret n° 2020-1512 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 ont tous un intérêt personnel à solliciter l'annulation du décret attaqué en tant qu'il autorise la collecte des opinions politiques, des convictions philosophiques, religieuses, syndicales, ainsi que celles relatives à l'activité sur les réseaux des groupements et personnes morales.

Parce qu'ils sont eux-mêmes susceptibles de voir les données concernant leur groupement, ou les dirigeants de leurs groupements, collectées et enregistrées, les exposants disposent donc un intérêt personnel à agir.

8. En leur qualité d'organismes dédiés à la défense et à la promotion des intérêts de leurs membres, les exposants disposent également d'un intérêt à agir contre le décret attaqué dans la mesure où le traitement automatisé de données modifié par le décret attaqué autorise l'enregistrement et la collecte d'informations sensibles, tenant notamment à des données subjectives comme celles qui ont trait aux opinions politiques, philosophiques, ou aux convictions syndicales, ceci sans le moindre encadrement.

9. En particulier, 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.

En tant que le décret attaqué affecte l'intérêt de leurs membres par leur caractère discriminant, leur liberté d'opinion et, par-là, les libertés publiques et individuelles en faveur desquelles les syndicats, fédérations et

unions de syndicats exposants se sont donnés pour mission d'œuvrer, ses 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.

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).

10. 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, le décret modifie un outil de gestion à disposition des agents de la gendarmerie nationale pour les besoins notamment des procédures judiciaires, et prévoit que les données ont pour destinataires notamment les procureurs de la République. Ce traitement affecte ainsi les conditions d'exercice des magistrats, et plus précisément des magistrats du parquet qui sont en charge de la direction des enquêtes et du contrôle des gardes à vue.

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 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 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.

11. 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.

Le fichier litigieux a en effet 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. Or le fichier EASP qui sera consulté indique si la personne concernée est recensée dans les fichiers PASP ou GISPAP.

La recevabilité de la requête est donc acquise.

II] Sur l'illégalité du décret

A] Sur l'illégalité externe du décret

12. La légalité externe du décret présente un doute sérieux dès lors que son adoption n'a pas fait l'objet d'une consultation régulière de la CNIL (**A.1**) ni du Conseil d'Etat (**A.2**) et dès lors que son adoption n'a pas été précédée d'une analyse d'impact (**A.3**).

A.1] Sur l'irrégularité de la consultation de la CNIL

13. 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* ».

Par ailleurs, aux termes du II de l'article 31 de la même loi :

> « *II.- Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement.* »

Les dispositions du I de l'article 6 de la loi du 6 janvier 1978 interdisent le traitement des données à caractère personnel qui révèlent notamment les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou des données concernant la santé d'une personne physique et il ne peut être dérogé à cette interdiction que par décret en Conseil d'Etat pris après avis motivé et publié de la CNIL.

Le Conseil d'Etat juge à cet égard que l'organisme dont une disposition législative ou réglementaire prévoit la consultation avant l'intervention d'un texte doit être mis à même d'exprimer son avis sur l'ensemble

des questions soulevées par ce texte et que, dans le cas où, après avoir recueilli son avis, l'autorité compétente pour prendre ledit texte envisage d'apporter à son projet des modifications qui posent des questions nouvelles, elle doit le consulter à nouveau (CE, 30 décembre 2009, *association SOS Racisme*, n° 312051, publié au Lebon).

Le décret ne peut donc pas contenir de dispositions qui diffèrent à la fois du projet initial du gouvernement et des recommandations faites par la CNIL, lorsque ces dispositions posent des questions nouvelles qui justifieraient une seconde consultation de la CNIL.

14. Or, le projet de décret qui a été adopté n'est pas celui qui a été soumis à la CNIL et comporte des éléments nouveaux qui exigeaient une nouvelle consultation de cette commission.

Il en va ainsi de la collecte de données relatives aux opinions politiques, aux convictions philosophiques, religieuses ou à l'appartenance syndicale d'une part (i), et de la mise en œuvre d'un dispositif d'interrogation par la photographie d'autre part (ii).

(i) ***Sur le défaut de consultation quant à la collecte de données relatives aux opinions politiques, aux convictions philosophiques, religieuses ou à une appartenance syndicale***

15. Dans sa rédaction antérieure à la publication du décret attaqué, issue du décret du 4 décembre 2013, l'article R. 236-23 du code de la sécurité intérieure disposait que :

> *«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. 236-21.*
> *Par dérogation, sont autorisés, pour les seules fins et dans le strict respect des conditions définies à la présente section, la collecte, la conservation et le traitement de données concernant les personnes mentionnées à l'article R. 236-21 et relatives :*
> *1° A des signes physiques particuliers et objectifs comme éléments de signalement des personnes ;*
> *2° A des activités politiques, philosophiques, religieuses ou syndicales.*
> *Il est interdit de sélectionner dans le traitement une catégorie*

particulière de personnes à partir de ces seules données» (soulignement ajouté).

L'article 3 du décret attaqué a modifié ces dispositions qui prévoient désormais que :

«L'interdiction prévue au I de l'article 6 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. 236-21.
Par dérogation, sont autorisés, pour les seules fins et dans le strict respect des conditions définies à la présente section, la collecte, la conservation et le traitement de données concernant les personnes mentionnées à l'article R. 236-21 et relatives :
1° A des signes physiques particuliers et objectifs comme éléments de signalement des personnes ;
2° A des opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale ;
3° A des données de santé révélant une dangerosité particulière.
Il est interdit de sélectionner dans le traitement une catégorie particulière de personnes à partir de ces seules données. (soulignement ajouté).

L'article 3 du décret attaqué a ainsi autorisé la collecte de données relatives aux opinions politiques, des convictions philosophiques, religieuses ou syndicales en lieu et place des données relatives aux activités politiques, philosophiques, religieuses ou syndicales.

Pourtant, le projet de décret qui a été soumis à la CNIL ne mentionnait pas cette substitution et se bornait à indiquer que l'article 3 du décret ajouterait aux dispositions précitées de l'article R. 236-23 du code de la sécurité intérieure les seules données de santé révélant une dangerosité particulière.

A ce titre, l'avis de la CNIL sur l'article 3 du projet de décret se limite à mentionner les conséquences tenant à l'ajout des données de santé révélant une dangerosité particulière, sans se prononcer sur les conséquences du traitement de données relatives aux opinions politiques, ou aux convictions philosophiques, religieuses ou syndicales :

« Sur les données collectées
A titre liminaire, la Commission relève que la rédaction de certaines catégories de données est particulièrement large. Si elle ne remet pas en cause la difficulté de préciser de manière exhaustive l'ensemble des données pouvant être collectées à ce titre, au regard notamment des nécessités opérationnelles propres à chaque situation, elle estime toutefois qu'à certains égards, le projet de décret pourrait être précisé afin de délimiter de manière plus fine ce que recoupent ces catégories.

> *En premier lieu, l'article 3 du projet de décret prévoit que des « données de santé révélant une dangerosité ou une vulnérabilité particulière » peuvent faire l'objet d'une collecte. A ce titre, des données portant sur des « troubles psychologiques ou psychiatriques connus ou signalés dans le mesure où ces données sont strictement nécessaires à l'évaluation de la dangerosité » peuvent faire l'objet d'une collecte.*
> *A cet égard, la Commission prend acte que les informations ainsi collectées se limitent à la description des troubles et de l'éventuel suivi psychiatrique d'une personne, à l'exclusion de toute donnée fournie par un professionnel de santé soumis au secret médical.*
> *Elle rappelle néanmoins que la mention de ces informations revêt un caractère sensible. En effet, ces informations constituent des données de santé au sens de la réglementation applicable en matière de protection des données à caractère personnel, qui doivent faire l'objet d'une vigilance renforcée. Si la collecte de ces données n'appelle pas d'observation particulière, elle souligne que toute information qui serait couverte par le secret médical devrait, en outre, bénéficier, sauf disposition contraire, de la protection prévue à l'article L. 1110-4 du code de la santé publique.*
> *En deuxième lieu, l'article 2 du projet de décret prévoit que les « identifiants utilisés sur les réseaux sociaux » ou les « activités sur les réseaux sociaux » peuvent faire l'objet d'une collecte au sein du traitement»* (délibération n° 2020-065 du 25 juin 2020 de la CNIL) (**production n°2**).

La CNIL n'a pas été consultée sur la substitution opérée par l'article 3 du décret attaqué précisément parce que le projet de décret qui lui a été soumis ne comportait pas cette modification, et ce manquement a d'ailleurs été confirmé par voie de presse où les membres de la CNIL indiquent ne pas avoir été consultés sur ce point :

> *«En outre, les "opinions politiques" et les "convictions philosophiques et religieuses" pourront également être recensées, et plus seulement les "activités" politiques ou religieuses. Sur ce point, Marion de Gasquet, juriste à la Cnil, précise à franceinfo que la Commission n'a pas été consultée, ces modifications ayant été apportées après la délibération du gendarme des données personnelles. Le ministère de l'Intérieur indique qu'il ne s'agit "que d'une évolution terminologique" qui "recouvre les mêmes réalités". "Collecter des données sur une activité politique ou religieuse conduit par définition à préciser la nature de cette opinion", affirme-t-on place Beauvau»* (A. GALOPIN - Franceinfo, *Opinions politiques, pratiques sportives, données de santé... Les possibilités de fichage élargies par trois décrets publiés en toute discrétion,* article du 9 décembre 2020 12h50) (**production n° 3**).

En tant qu'il ajoute à l'article R. 236-23 du code de la sécurité intérieure la possibilité de collecter de données relatives aux opinions politiques, aux convictions philosophiques, religieuses ou syndicales, le décret attaqué

contient des dispositions qui n'était pas intégrées dans le projet initial soumis pour consultation à la CNIL et qui n'ont pas été soumises à une nouvelle consultation de la CNIL.

16. Loin d'être purement terminologique, cette modification affecte l'économie générale des données susceptibles d'être collectées sur ce fondement.

Les données relatives aux activités politiques, philosophiques, religieuses ou syndicales renvoient exclusivement à l'exercice de fonctions ou de responsabilités telles que l'exercice d'une fonction politique au sein d'un parti politique, l'exercice d'une fonction religieuse, l'exercice d'une responsabilité dans une association déclarée ou d'un mandat syndical.

Or, l'exercice d'une telle activité révèle de la part de l'intéressé un engagement qui excède le cadre de sa vie privée puisqu'elle se caractérise par une exhibition d'une revendication ou d'une conviction, ce qui a pour effet de diminuer l'intensité de la protection habituellement réservée aux opinions ou aux convictions politiques, religieuses ou syndicales (A. ILJIC, conclusions lues sous : CE, 14 novembre 2018, n° 409936). Le juge judiciaire considère pour ce motif que la révélation de l'exercice de fonctions et de responsabilité ou de direction au titre d'une quelconque appartenance politique religieuse ou philosophique ne constitue pas une atteinte à la vie privée (Civ., 1e, 12 juillet 2005, n° 04-11.732, Bull. n° 329, p. 272).

Dès lors qu'elles renvoient à deux réalités distinctes et qu'elles ne bénéficient pas de la même protection, les données relatives aux activités politiques, philosophiques, religieuses ou syndicales se distinguent substantiellement des opinions politiques, des convictions philosophiques, religieuses ou syndicales.

Pourtant, on l'a vu, le gouvernement n'a pas consulté la CNIL sur l'autorisation de collecter des données relatives aux opinions politiques, et aux convictions philosophiques, religieuses ou syndicales en lieu et place des données relatives aux activités politiques, philosophiques, religieuses ou syndicales.

Ce manquement est d'autant plus grave qu'il concerne précisément des données dont le traitement, par principe prohibé, est soumis à l'édiction d'un décret pris sur consultation préalable de la CNIL.

Faute pour le Premier ministre d'avoir régulièrement consulté la CNIL, le décret attaqué méconnaît les articles 8 et 31 de la loi du 6 janvier 1978.

(ii) ***Sur l'absence de consultation sur le dispositif d'interrogation par la photographie***

17. Dans sa délibération en date du 25 juin 2020, la CNIL relevait que l'article 2 du projet de décret prévoyait la possibilité d'effectuer une recherche à partir des photographies enregistrées dans le traitement et indiquait à cet égard :

> « *Sans remettre en cause le principe de la mise en œuvre d'un tel dispositif, elle s'interroge, en l'absence de précisions sur ce point, sur les caractéristiques techniques du futur dispositif et sur les données qui seront nécessaires à son fonctionnement. Elle estime notamment que, dans le cas où le dispositif utiliserait un gabarit biométrique, celui-ci constituerait en lui-même une donnée relevant d'une catégorie distincte de celles listées dans le projet de décret. Dans cette hypothèse, le déploiement de ce mode d'interrogation du fichier nécessiterait donc la modification de l'article R. 236-22 du code de la sécurité intérieure, après saisine de la Commission, dans les conditions prévues à l'article 31 de la loi du 6 janvier 1978 modifiée* » (délibération n° 2020-065 du 25 juin 2020 de la CNIL) (**production n°2**) (soulignement ajouté).

Dans sa version définitive, le décret adopté a confirmé la possibilité d'effectuer une recherche à partir des photographies enregistrées dans le traitement puisque son article 2 a supprimé la mention «*le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie*», jusqu'alors inscrite au dernier alinéa de l'article R 236-22 du code de la sécurité intérieure.

En supprimant cette interdiction, le décret attaqué a introduit la possibilité d'introduire dans le traitement un dispositif de reconnaissance faciale à partir de la photographie et ainsi de mettre en œuvre une technique utilisant un gabarit biométrique.

Le Premier ministre a modifié sur ce point l'article R. 236-22 du code de la sécurité intérieure mais il n'a pas consulté la CNIL, alors même qu'elle en avait formulé l'exigence dans son avis précité.

Sous cet angle encore, les dispositions de l'article 8 de la loi du 6 janvier 1978 ont été méconnues.

18. Faute pour le Premier ministre d'avoir régulièrement consulté la CNIL, le décret attaqué a été adopté en méconnaissance des règles qui gouvernent l'examen par la CNIL des projets de décrets.

De ce premier chef, l'annulation s'impose.

A.2] Sur la consultation irrégulière du Conseil d'Etat

19. On l'a vu, il ressort des dispositions du II de l'article 31 de la loi du 6 janvier 1978 que les traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission.

Le décret autorisant la mémorisation de données sensibles 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.

Surtout, compte tenu de ce qui précède, il peut être redouté que la version du projet de décret qui a été transmise au Conseil d'Etat soit identique à celle transmise à la CNIL et qu'elle soit en conséquence incomplète. La nécessité d'un examen comparatif s'impose d'autant plus ici que les dispositions du texte litigieux appellent un contrôle très strict du point de vue de leur objet, de la finalité des fichiers, de la nature des informations traitées, de leur sensibilité, et de l'importance de leur impact sur la vie privée et les libertés individuelles ou publiques.

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

L'annulation est encourue.

A.3] Sur l'absence préalable de réalisation d'une étude d'impact

21. La directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 est applicable aux traitements utilisés par les forces de l'ordre en matière de justice à l'exclusion de ceux dédiés à la protection de la sûreté de l'Etat.

L'article 27 de cette directive prévoit en son premier alinéa que :

> « *Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel* ».

Une analyse d'impact est exigée en présence d'un traitement recourant à une technologie nouvelle compte tenu de la sensibilité des données concernées et de leur impact sur la vie privée et dans la mesure où une telle étude permet d'établir les risques de son déploiement.

Le juge des référés du Conseil d'Etat a ainsi retenu que la méconnaissance de l'obligation de procéder à une telle analyse suffisait à elle-seule à entraîner l'illégalité du traitement (CE, Ord., 26 juin 2020, *Ligue des droits de l'homme*, n° 441065).

22. Dans le cas présent, le traitement dont il est question n'intéresse que pour partie la sûreté de l'Etat puisqu'il poursuit une double finalité : d'une part, il concerne des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sûreté de l'Etat et, d'autre part, il vise des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique.

En vertu de cette dernière finalité, il est soumis aux dispositions de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, et à son article 27 dont il a été vu qu'il impose une analyse d'impact préalable.

On l'a vu, dans sa version définitive, le décret adopté a confirmé la possibilité d'effectuer une recherche à partir des photographies enregistrées dans le traitement puisque son article 2 a supprimé la mention «*le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie*», jusqu'alors inscrite au dernier alinéa de l'article R 236-22 du code de la sécurité intérieure.

Et, faute de distinguer les finalités poursuivies, le décret n'a pas réservé la possibilité d'utiliser un dispositif de reconnaissance faciale à partir de la photographie pour les seules personnes dont les données sont collectées à raison de la menace qu'elles sont susceptibles de constituer pour la sûreté de l'Etat. De la sorte, le moyen pris de la méconnaissance de l'article 27 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 est par conséquent opérant.

Or, la possibilité d'effectuer une recherche à partir des photographies enregistrées dans le traitement implique la mise en œuvre une technique utilisant un gabarit biométrique, si bien que le décret litigieux devait faire l'objet d'une analyse d'impact préalable.

C'était d'ailleurs précisément l'objet de la recommandation de la CNIL qui avait indiqué qu'elle « *elle s'interroge, en l'absence de précisions sur*

ce point, sur les caractéristiques techniques du futur dispositif et sur les données qui seront nécessaires à son fonctionnement » et qu'elle « *demande à être rendue destinataire de tout élément permettant d'apprécier les modalités, notamment techniques, de mise en œuvre de cette fonctionnalité, ainsi que l'analyse d'impact relative à la vie privée des données mise à jour et ce, avant sa mise en œuvre effective* » (délibération n° 2020-065 du 25 juin 2020 de la CNIL).

Faute pour le décret d'avoir été précédé d'une analyse d'impact du dispositif permettant d'effectuer une recherche à partir des photographies enregistrées dans le traitement, celui-ci méconnaît les dispositions de l'article 27 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016.

L'annulation est inéluctable.

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

23. 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 98 de cette même loi du 6 janvier 1978 (**B.3.**), et de ce que les dispositions qui permettent spécifiquement la collecte et le traitement de données visées par l'article 6 de la loi précitée méconnaissent l'article 88 de cette loi, ensemble les droits et libertés précités (**B.4.**).

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**

24. 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.

25. 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.

26. Dans le cas présent, 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 :

- l'absence de finalité claire et légitime donnée au traitement litigieux (**B.1.1.**)
- du caractère inadéquat et non pertinent des données collectées (**B.1.2.**)
- du périmètre excessivement étendu de l'accès aux données (**B.1.3.**)
- du caractère excessif de la durée de conservation des données (**B.1.4.**).

B.1.1. Sur l'absence de finalité claire et légitime donnée au traitement litigieux

27. Par définition, un traitement automatisé de données personnelles correspond à «*un ensemble cohérent d'opérations techniques concourant à la même finalité*» (A. LALLET, conclusions lues sous : CE, 27 mars 2020, *CRPA*, n° 431350, mentionné aux tables) (soulignement ajouté).

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).

Et, c'est également 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.

Il suit de là qu'un traitement automatisé de données personnelles peut comprendre plusieurs opérations qui doivent toutes répondre à une finalité analogue puisque c'est au regard de celle-ci que sera appréciée la proportionnalité de l'ingérence dans l'exercice du droit au respect de la vie privée.

28. Ensuite, l'article 4 de la loi n°78-17 du 6 janvier 1978 prévoit que les données personnelles ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes. Ces deux premières exigences impliquent que la finalité attachée au traitement doit d'abord être énoncée de manière suffisamment précise de façon à encadrer l'usage qui sera fait du traitement et à neutraliser tout risque d'usage excessif.

C'est en effet 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).

L'exigence de légitimité quant à elle que le traitement réponde à une nécessité réelle, de sorte qu'il ne peut pas être mis en œuvre pour l'obtention de données déjà susceptibles d'être récoltées par des fichiers existants (Cons. Const., 27 décembre 2019, décision n° 2019-796 DC, loi de finances pour 2020, cons. 94 ; V. également : A. BRETONNEAU, concl. lues sous : CE, 21 septembre 2015, *association de défense et d'assistance juridique des intérêts des supporters et autres*, n°389815, mentionné aux tables).

29. Pour mémoire, le «GIPASP» avait uniquement vocation à collecter les informations des personnes physiques susceptibles de porter atteinte à la sécurité publique et en particulier celles des personnes susceptibles d'être

impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives.

L'article premier du décret attaqué étend d'abord cette finalité aux personnes morales et aux groupements.

Ce même article ajoute surtout une nouvelle finalité à ce traitement qui a désormais vocation à collecter les informations des personnes physiques ou morales, ainsi que des groupements dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou à la sûreté de l'Etat. L'article R 236-21 du code de la sécurité intérieure dispose à cet égard que :

> «*Le traitement a notamment pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes susceptibles de prendre part à des activités terroristes, de porter atteinte à l'intégrité du territoire ou des institutions de la République ou d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives.*
> *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*».

En raison de l'évolution résultant du décret attaqué, le fichier ne présente plus de finalité claire en raison du cumul de deux finalités et de la confusion qui en résulte (i) et l'existence d'autres traitements pour la sûreté de l'Etat le prive de sa finalité légitime (ii).

(i) Sur l'absence de finalité claire du traitement en raison du cumul de deux finalités et de la confusion qui en résulte

30. On l'a vu, le traitement doit répondre à une même finalité, c'est-à-dire une finalité homogène à la lumière de laquelle sera appréciée la légalité de l'ingérence dans l'exercice du droit au respect de la vie privée. C'est en effet au regard de cette finalité que sera appréciée la proportionnalité du paramétrage du traitement (nature des données collectées, durée de la conservation des données, droit des personnes visées).

Or, dans le cas présent, le décret attaqué assigne au GIPASP une nouvelle finalité parfaitement étrangère à celle qu'il poursuivait initialement, de sorte qu'aujourd'hui ce traitement poursuit deux finalités totalement différentes qui doivent générer un cadre juridique distinct :

- d'une part, la première finalité concerne des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique et en particulier les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives. Le traitement relève à cet égard 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.

- d'autre part, la seconde finalité concerne des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sûreté de l'Etat, c'est-à-dire celles qui sont susceptibles de prendre part à des activités terroristes et de porter atteinte à l'intégrité du territoire ou des institutions de la République. Le traitement relève à ce titre des seules dispositions spécifiques de la loi n°78-17 du 6 janvier 1978.

Le décret litigieux prétend ainsi regrouper sous un fichier unique plusieurs bases de données informatiques et fichiers de données à caractère personnel répondant à des finalités de nature parfaitement distincte puisque seule la seconde finalité permet de ranger le traitement au nombre de ceux qui intéressent la sûreté ou la sécurité publique.

Or, rien ne justifie que la prévention contre les menaces à la sécurité publique puisse conduire à centraliser des renseignements étrangers à cet objectif sous la bannière de la sûreté de l'Etat, sauf à engendrer des risques d'arbitraires accrus à raison de la confusion des deux finalités en un traitement unique.

La CNIL avait d'ailleurs à cet égard relevé que «*le traitement GIPASP vise à prévenir des atteintes de nature très diverses qui peuvent dès lors porter sur des agissements ou des individus n'étant pas susceptibles de porter atteinte à la sûreté de l'Etat*» car «*le traitement n'intéresse que pour partie la sûreté de l'Etat*» (délibération n° 2020-065 du 25 juin 2020).

Le décret prévoit ainsi de cumuler deux finalités qui à elles-seules permettent la collecte de très nombreuses données, et il résulte de ce cumul une extension excessive des données susceptibles d'être collectées dont le périmètre est trop large pour répondre à une finalité claire et précise.

Il suit de là que de par la nouvelle finalité qu'il assigne au GIPASP, le décret attaqué octroie à ce traitement une finalité qui n'est plus homogène et qui à l'évidence est manifestement trop large.

31. A cela s'ajoute la circonstance que les règles de mise en œuvre du traitement ne distinguent pas l'une ou l'autre des deux finalités poursuivies.

Compte tenu de la diversité des finalités poursuivies et de l'étendue des données susceptibles d'être collectées, la CNIL estimait «*indispensable que des mesures soient mises en œuvre afin de permettre de distinguer de manière précise les données ayant vocation à être traitées pour des finalités relevant de la sûreté de l'Etat* » (délibération n° 2020-065 du 25 juin 2020).

La commission reprochait ainsi au décret de ne pas introduire de distinction selon la finalité poursuivie s'agissant tant de la nature des données collectées, que de l'exercice par les personnes concernées de leurs droits :

> *« 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° 2020-065 du 25 juin 2020).

Force est cependant de constater que la CNIL n'a pas été entendue et que le décret s'abstient de dissocier pour la collecte des données, comme pour leur enregistrement, les finalités poursuivies par le traitement, de sorte qu'on peut redouter que les données en principe collectées pour la sûreté de l'Etat nourrisse finalement le renseignement pour la sécurité publique.

Le décret permet ainsi la collecte de données personnelles pour certaines d'une sensibilité accrue sans préciser que certaines de ces données ne peuvent être collectées et enregistrées que lorsque l'individu concerné est susceptible de porter atteinte à la sûreté de l'Etat.

Concrètement, les données relatives à l'état de santé, aux troubles psychologiques, aux opinions politiques, ou aux convictions religieuses pourront être collectées de la même façon pour un individu radicalisé dont le comportement porte atteinte à la sûreté de l'Etat ou pour un individu connu pour avoir participé à des violences urbaines dans le cadre d'une manifestation ou en qualité de supporter d'une équipe de football.

Ensuite, s'agissant du traitement des données ainsi collectées, il soumet à un seul et unique régime les données des personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives et celles qui celles qui sont susceptibles de prendre part à des activités terroristes et de porter atteinte à l'intégrité du territoire ou des institutions de la République.

A titre d'illustration, et ainsi qu'il sera vu, ces données peuvent être conservées pour une même durée de dix ans indépendamment de la finalité motivant leur enregistrement, et le décret ne distingue pas plus les destinataires de ces données en raison de la finalité poursuivie.

Cette confusion entre les données collectées au titre de l'une ou de l'autre des finalités poursuivies 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.

Elle conduit ainsi à un mélange des genres et un amalgame gravement préjudiciable aux droits des personnes visées comme au respect de leur vie privée.

La licéité du traitement s'en trouve inéluctablement affectée puisque le regroupement et la centralisation en un traitement unique de fichiers mis en œuvre pour des finalités de nature aussi différente, relevant au demeurant d'un droit positif différent, fait obstacle à ce que ces finalités soient regardées comme déterminées, explicites et légitimes.

(ii) Sur l'absence de finalité légitime du traitement du fait de l'existence d'autres traitements dédiés à la sûreté de l'Etat

32. L'absence de légitimité du traitement contesté résulte de son absence de nécessité au regard des outils dont disposent d'ores et déjà les services de la gendarmerie nationale pour la sûreté de l'Etat.

L'article R. 841-2 du code de la sécurité intérieure recense vingt-huit traitements automatisés de données à caractère personnel intéressant la sûreté de l'Etat autorisés par les actes réglementaires, c'est-à-dire des traitements relevant de la politique de renseignement qui, pour reprendre les termes de l'article L. 811-1 du code de la sécurité intérieure, visent à « *concourir à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation* ».

Parmi eux, plusieurs sont mis en œuvre par la direction générale de la gendarmerie nationale, et il en va notamment ainsi du traitement ACCReD (automatisation de la consultation centralisée de renseignements et de données), ou du fichier des personnes recherchées autorisé par décret n° 2010-256 du 28 mai 2010.

Dès lors que plusieurs traitements accessibles aux services de gendarmerie ont déjà pour finalité la collecte d'informations relatives aux personnes dont l'activité indique qu'elles peuvent porter atteinte à la sûreté de l'Etat, il aurait été plus approprié de modifier ces traitements déjà existants plutôt que d'associer comme le fait le décret attaqué, un nouveau traitement à un traitement dont la finalité est parfaitement étrangère à la sûreté de l'Etat.

La modification par les dispositions litigieuses du traitement GIPASP étant par conséquent surabondante au regard des autres traitements existants, l'exigence de légitimité n'est pas satisfaite et l'ingérence qui en résulte

dans le droit au respect de la vie privée des personnes intéressées n'est pas proportionnée.

Partant, en tant qu'il assigne au traitement une nouvelle finalité étrangère à la première, et en tant que cette jonction génère une confusion, le décret litigieux lui a fait perdre sa finalité claire et légitime et a supprimé, dans le même temps, la pertinence des informations recueillies au regard de la finalité poursuivie.

B.1.2. Sur le caractère inadéquat et non pertinent des données collectées

33. 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.

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

35. 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.

36. Dans le cas présent, les articles 2 et 3 du décret attaqué prévoient de manière assez classique que les données ne sont susceptibles d'être collectées que dans la stricte mesure où elles sont nécessaires, ou pour les seules fins et dans le strict respect des conditions définies par les dispositions de la section.

S’agissant des personnes concernées par la collecte, l’article 2 du décret ne limite pas l’enregistrement des données des seules personnes pouvant porter atteinte à la sécurité publique ou à la sûreté de l'Etat mais il l’étend également :

- aux personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne pouvant porter atteinte à la sécurité publique ou la sûreté de l'Etat,
- aux victimes des agissements de la personne physique pouvant porter atteinte à la sécurité publique ou la sûreté de l'Etat,
- aux personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne morale ou le groupement pouvant porter atteinte à la sécurité publique ou à la sûreté de l'État,
- aux victimes des agissements de ces personnes morales et groupements.

Plus déroutantes encore sont les dispositions qui fixent les nouvelles données susceptibles d’être enregistrées dans ce traitement.

L’article 2 autorise ainsi, s’agissant de la personne physique pouvant porter atteinte à la sécurité publique ou à la sûreté de l'Etat, 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.

L'article 3 ajoute à ces données, concernant spécifiquement les personnes susceptibles de porter atteinte à la sûreté de l'Etat et les personnes susceptibles de porter atteinte à la sécurité publique, celles relatives à des opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale ainsi que les données de santé révélant une dangerosité particulière.

De manière générale, ces données ne sont ni pertinentes (i), ni adéquates (ii) et le périmètre des individus concernés par la collecte est manifestement excessif (iii).

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

37. D'abord, le décret autorise la collecte de données extrêmement étendues, pour certaines sensibles, ceci sans opérer de distinction selon la nature de la menace présentée par la personne intéressée et, donc, selon la finalité du traitement poursuivie.

Sous couvert de sûreté de l'Etat, le décret litigieux permet de rassembler des informations extrêmement sensibles – relatives aux opinions politiques, philosophiques, syndicales, religieuses comme des données de santé, relatives aux addictions, aux troubles psychologiques ou psychiatriques – alors qu'elles seraient collectées sur des personnes qui ne présenteraient pas de menace pour la sûreté de l'Etat mais seulement pour la sécurité publique.

Ainsi, le décret permet la collecte d'informations relatives aux opinions, aux convictions, à l'appartenance religieuse, à l'état de santé, aux troubles psychologiques, aux relations, ou à l'activité sur les réseaux sociaux d'individus mis en cause pour des faits de violence collective à l'occasion de manifestations sportives, sans lien avec la sûreté de l'Etat.

Il s'agit là d'une pure logique de maximisation des informations qui plus est sans lien préétabli avec la protection de la sécurité publique, laquelle n'exige pas la collecte de telles données. Ce n'est pas parce que l'information semble pouvoir être collectée pour la sûreté de l'Etat que toute information de cette nature peut être collectée au titre de toute finalité de manière autonome.

Compte tenu du cumul de finalités, de la confusion qui en résulte, et de ce que les données sont collectées indifféremment de la menace que présente l'intéressé, le critère de la pertinence des données collectées n'est pas satisfait.

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

38. 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,
- «*les comportements et habitudes de vie*» sans plus de précision,
- «*les déplacements*» sans que le décret ne précise s'il s'agit des déplacement 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,
- «*des données relatives aux troubles psychologiques ou psychiatriques*» sans précision quant à la nature des troubles ou aux conditions d'obtention de ces données,
- «*aux facteurs familiaux, sociaux et économiques*», sans plus de précision.

L'article 3 du décret autorise ensuite la collecte :

- «*de données relatives aux opinions politiques, aux convictions philosophiques, religieuses et à l'appartenance syndicale*»
- « de « *données de santé révélant une dangerosité ou une vulnérabilité particulière* » ou de données portant sur des « *troubles psychologiques ou psychiatriques connus ou signalés* ».

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.

39. 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, le décret attaqué autorise la collecte de données d'une extrême sensibilité qui, du fait de leur nature subjective, ne répondent pas à l'exigence d'adéquation.

  L'auteur du décret n'a pas simplement autorisé 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 philosophiques politiques, syndicales 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 et intrusives génère un risque inhérent de discrimination et créé un climat de suspicion malsaine, ceci indépendamment de l'interdiction de sélection posée par le décret.

- **En deuxième lieu**, s'agissant des « *données de santé révélant une dangerosité ou une vulnérabilité particulière* » et de celles portant sur des « *troubles psychologiques ou psychiatriques connus ou signalés* » :

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, 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 de près ou de loin 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.

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

40. D'abord, le décret est parfaitement silencieux sur le cadre dans lequel pourront être collectées ces données et à quelles occasions et sur la nature des interactions (actions de prévention – investigations – ou interventions nécessaires à l'exercice des missions de polices judiciaire et administrative) qui justifieront que soient recueillies les données susceptibles d'alimenter le traitement.

Ensuite, le décret entend la collecte des données parmi les plus sensibles – celles de la catégorie 5° de l'article 2relatives aux activités, comportement de vie, activités sur les réseaux sociaux, pratique et comportement religieux – aux victimes ainsi qu'aux « *personnes en contact régulier et non fortuit avec la personne ou le groupement suivi* ».

Les dispositions litigieuses autorisent ainsi la collecte de données à raison de la seule fréquence des contacts qu'elles entretiennent avec des personnes dont les activités sont susceptibles de porter atteinte à la sécurité publique ou de porter atteinte à la sûreté de l'Etat.

De la sorte, n'importe quel individu qui entretient des contacts réguliers avec une personne visée par le traitement peut voir ses données – y compris celles extrêmement sensibles – collectées et ceci indépendamment du comportement de la personne concernée, de son statut, de sa mise en cause dans une procédure administrative ou pénale, ou de la menace qu'il représente.

Concrètement, le simple fait d'entretenir des contacts réguliers avec des individus mis en cause pour des faits de violence lors de manifestations permet la collecte de données extrêmement sensibles, alors que rien ne le justifie hormis la volonté de maximiser les données indépendamment de la menace présentée.

Au surplus, aucune exception n'est prévue pour tenir compte du secret dont bénéficient les personnes qu'il s'agisse notamment du secret de l'avocat ou du secret médical.

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 treize 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.

41. En définitive, 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 étendu 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

42. 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).

43. Dans le cas présent, l'article 6 prévoit que «*dans la limite du besoin d'en connaître, peuvent être destinataires des données* » :

- les personnes ayant autorité sur les services ou unités ayant accès aux données enregistrées dans le traitement, conformément aux dispositions en vigueur de l'article R. 236-16 du code de la sécurité intérieure.
- les procureurs de la République
- les agents d'un service de la police nationale ou d'une unité de gendarmerie nationale chargés d'une mission de renseignement et les

agents des services mentionnés aux articles R. 811-1 et R. 811-2 du code de la sécurité intérieure, sur autorisation expresse

- les personnels de la police nationale ou les militaires de la gendarmerie nationale qui ne sont pas chargés d'une mission de renseignement sur demande expresse, précisant l'identité du demandeur, l'objet et les motifs de la consultation.

Ainsi que le montre le dernier item, le décret attaqué étend 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.

Alors qu'il était déjà accessible à près de 84.000 agents, ce sont désormais 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 les opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale comme les données de santé.

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, le nombre de destinataires potentiel est strictement identique suivant que la personne est fichée parce qu'elle présente une menace pour la sécurité publique ou pour la sûreté de l'Etat.

Faute pour le décret d'établir une corrélation entre les destinataires et la finalité poursuivie par le traitement, ou d'instituer une distinction selon que les données collectées concernent la personne qui présente une menace ou la personne avec laquelle elle entretient des relations directes ou non fortuites, il permet à un agent de police qui sollicite un simple renseignement dans le cadre d'une mission relative à la seule sécurité publique d'obtenir des éléments d'information recueillis pour la sûreté de l'Etat.

En outre, et ainsi que l'a relevé la CNIL, 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.

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

44. 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).

48. 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.

49. Dans le cas présent, l'article R. 236-24 du code de la sécurité intérieure prévoit que les données collectées peuvent être conservées pendant une durée de dix ans après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ou à la sûreté de l'Etat ayant donné lieu à un enregistrement, et l'article R. 236-25 du même code réduit cette durée à trois ans pour les données concernant des mineurs.

D'abord, ces dispositions fixent une durée de conservation identique selon que la personne représente une menace pour la sécurité publique, la sûreté de l'Etat, ou qu'elle figure dans le traitement du fait de sa qualité de victime ou de tiers entretenant des contacts fréquents avec une personne représentant une menace. Pour le dire autrement, là encore, les individus ne présentant aucune menace sont soumis au même régime que les autres individus.

Ensuite, en tant qu'elles prévoient que cette durée court à compter de l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ou à la sûreté de l'Etat, les dispositions

réglementaires prévoient un cumul de la durée de conservation qui court pour une nouvelle durée de dix ans ou de trois à chaque intervention d'un nouvel évènement.

Enfin, faute pour le décret de distinguer selon la finalité poursuivie, le décret autorise la reconduction de la durée de conservation à raison de l'intervention d'un événement inhérent à une autre finalité que celle qui avait conduit initialement au fichage de l'intéressé.

Concrètement, un individu fiché à raison de ses signes de radicalisation verra la durée de conservation de ses données prolongée à 20 ans si à l'issue d'un délai de dix ans, il fait l'objet d'une interpellation à raison de violences commises dans un stade ou lors d'une manifestation.

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

45. Il faut ajouter à cela que le décret attaqué autorise le rapprochement du GIPASP avec d'autres traitements.

L'article 7 du décret attaqué prévoit à cet égard que :

> «*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).
> a

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 » ;
- 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 GIPASP et d'autres traitements de données, la durée de conservation des données enregistrées dans le GIPASP 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 « GIPASP » excède en conséquence ce qui est nécessaire pour la mise en œuvre de l'une et de l'autre des finalités assignées 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

46. 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

47. 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 quadruple exigence puisqu'elles prévoient que les données doivent être collectées pour des finalités déterminées explicites et légitimes (i), qu'elles 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).

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

- la finalité donnée au traitement litigieux n'est ni déterminée ni légitime en raison du cumul de deux finalités et de la confusion qui en résulte,
- 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.

B3] **<u>Sur la méconnaissance de l'article 98 de la loi n° 78-17 du 6 janvier 1978 et de l'article 6 de la directive n° 2016/680 du 27 avril 2016</u> à <u>raison de l'absence de distinction selon la gravité de la menace présentée par l'individu</u>**

49. Si la Cour européenne des droits de l'homme reconnaît que l'intérêt de la collectivité à voir protégées les données personnelles peut parfois s'effacer devant l'intérêt légitime que constitue la prévention des infractions pénales, elle souligne d'une part que de tels dispositifs ne sauraient être mis en œuvre dans une logique excessive de maximisation des informations (CEDH, 22 juin 2017, *Aycaguer c. France*, n° 8806/12, §34) et, d'autre part, qu'il y a lieu d'être particulièrement attentif au risque de stigmatisation des personnes non reconnues coupables d'infraction dans la mesure où si la conservation de données n'équivaut pas à l'expression d'un soupçon, il demeure que ce type de mention peut donner aux intéressés l'impression de ne pas être considérés comme innocent, et peut nuire à leur réputation ou rendre plus difficile leur quotidien (CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Unis*, §122 ; CEDH, 18 octobre 2011, *Khelili c. Suisse*, n° 16188/07, §64 ; CEDH, 18 septembre 2014, *Brunet c. France*, n°21017/10, §37).

Elle en déduit que le dispositif ne peut traiter de manière égale les données des coupables des infractions les plus graves et les moins graves ou encore celles des victimes ou des individus présumés innocents, et considère en conséquence que méconnaît ces règles le traitement qui ne prévoit aucune différentiation entre la nature et la gravité de l'infraction commise, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière (CEDH, 4 décembre 2008, *S. et Marper c. Royaume-Unis*, §119 ; CEDH, 18 avril 2013, *M. K. c. France*, n° 19522/09, §41 ; CEDH, 18 septembre 2014, *Brunet c. France*, n°21017/10, §119 ; CEDH, 22 juin 2017, *Aycaguer c. France*, n° 8806/12, §43).

De la même manière, le Conseil constitutionnel a censuré les dispositions qui prévoyaient la prolongation de la conservation des données au motif que cette prolongation était autorisée indépendamment de la gravité des faits (Cons. Const. 11 mars 2011, décision n° 2011-625 DC, cons. 72).

Ces exigences ont été reprises par l'article 6 de la directive n° 2016/680 du 27 avril 2016 et par l'article 98 de la loi du 6 janvier 1978, dont il ressort que le responsable de traitement établit, dans la mesure du possible et le cas échéant, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que : 1° les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou

sont sur le point de commettre une infraction pénale ; 2° les personnes reconnues coupables d'une infraction pénale ; 3° les victimes d'une infraction pénale, 4° les tiers à une infraction pénale.

50. L'ensemble des actes réglementaires autorisant des traitements à destination des forces de police ou de gendarmerie ont en commun d'instituer un régime particulier selon que les données concernent les auteurs d'infractions et, au sein de ceux-ci, selon la gravité de l'infraction.

A titre d'illustrations, le décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires comme le décret n° 2014-187 du 20 février 2014 relatif à la mise en œuvre de traitements de diffusion de l'information opérationnelle au sein des services et unités de la police et de la gendarmerie nationales distinguent la durée de conservation des données selon la gravité de l'infraction.

51. Dans le cas présent, le décret attaqué n'introduit aucune distinction entre les catégories de personnes qui permettrait de tenir compte de la nature de la menace qu'elles sont susceptibles de porter, du statut des personnes mises en cause, soupçonnés, ou coupables, ou de la nature de la procédure qui a conduit à la collecte des données.

Concrètement, la personne mise en cause dans une enquête pour des faits de terrorisme ou celle qui est interpellé au cours d'une manifestation créant un trouble à l'ordre public peuvent toutes deux voir collectées des données relatives à leurs opinions politiques, philosophiques ou syndicale, et les données sont soumises au même régime en terme de conservation, d'accès ou de durée de conservation. L'auteur du décret a ainsi autorisé la collecte des données personnelles les plus sensibles sans introduire une quelconque distinction suivant la catégorie des personnes concernées.

Et ce n'est pas tout.

Il en va de même de la durée de conservation des données qui là encore n'est pas limitée à une catégorie de personnes, personnes mises en cause, tiers ou victimes. Aussi, la participation à un parti politique d'une personne ne présentant aucune menace mais qui entretiendrait des contacts réguliers et non fortuits avec une personne susceptible de représenter une menace pour la sécurité

publique pourra faire l'objet d'une collecte pendant dix années alors que rien ne le justifie.

Le décret contesté répond en réalité à une logique de maximisation des informations, ceci indépendamment de la nature ou de la gravité de la menace qu'ils représentent.

A tout le moins, l'auteur du décret n'a pas pris soin de neutraliser ou à tout le moins limiter le risque de stigmatisation qui résulte de la collecte dans un fichier des données relatives aux opinions, à l'appartenance religieuse, à la santé de tout individu.

52. En tant qu'il a prévu un traitement uniforme des données personnelles de l'ensemble des individus sans introduire de distinction au regard du statut des individus ou de la gravité des infractions pour lesquelles ils seraient mis en cause, le décret attaqué a méconnu les dispositions de l'article 98 de la loi n° 78-17 du 6 janvier 1978 et celles de l'article 6 de la directive n° 2016/680 du 27 avril 2016.

L'annulation est encourue.

B.4] <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>

53. 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.

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

B.4.1] Sur l'absence de définition des cas de nécessité absolue

55. D'une part, l'article R. 236-22 du code de la sécurité intérieure dans sa rédaction issue du décret attaqué se limite à indiquer que la collecte des données collectées s'effectue « *dans la stricte mesure où elles sont nécessaires à la poursuite des finalités* », là où l'article R. 236-23 prévoit pour sa part que la collecte des données en principe interdites sont autorisés « *pour les seules fins et dans le strict respect des conditions définies à la présente section* ».

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 borné à se référer au strict respect des finalités poursuivies sans en décrire les circonstances et sans 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 introduit une dose d'arbitraire et de subjectivité

quant au point de savoir si les circonstances de l'espèce rendent strictement nécessaire la collecte des données.

B.4.2] Sur l'absence de garantie appropriée

56. 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 se limite à prévoir que ces données sont collectées dans la stricte mesure où elles sont nécessaires à la poursuite des finalités définies par le décret alors même qu'il a été démontré que le périmètre de ces finalités était manifestement trop large. De plus, il s'agit là encore de précisions abstraites et au demeurant ineffectives puisque le décret ne limite pas les missions au titre desquelles ces données d'une sensibilité accrue sont collectées.

En prévoyant à la fois comme limite et comme justification que les informations en cause soient nécessaires à l'exercice de la finalité poursuivie, les dispositions critiquées comportent une mention à caractère tautologique aussi insuffisante qu'inutile : celle-ci tend en effet à prévoir pour seule et unique garantie l'exclusion de l'exploitation des données en cause à des fins étrangères partisanes ou privées, ce que par définition la soumission du traitement litigieux au principe de légalité suffit en tout état de cause à garantir.

Rien n'exclut que des données sensibles soient enregistrées sans qu'elles ne soient nécessaires pour les finalités du fichier, et que les informations qui en constituent le support ne débordent pas des données objectives pour basculer dans des appréciations empreintes de préjugés. Nul ne peut concevoir, à ce jour que les pouvoirs publics puissent laisser à disposition des forces de l'ordre des outils leur permettant de manier des données d'une extrême sensibilité sans placer des gardes fous et des contrôles appropriés – à supposer que le principe d'une telle collecte puisse être admis, ce qui ne peut être le cas ici, ainsi qu'il a été démontré.

57. 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° 2020-1512 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° 2020-1512 du 2 décembre 2020
2 délibération n° 2020-065 du 25 juin 2020 de la CNIL
3 article de presse du 9 décembre 2020