447513, 447515, 447518 Ligue des droits de l'Homme et SFOIP
447969, 447971, 447973 CGT et autres
448059, 448048, 448051 La Quadrature du Net
449299, 449300, 449301 Conseil national des barreaux
449461, 449468, 449469 Collectivité territoriale de Corse et autres

10ème et 9ème chambres réunies

Séance du 3 décembre 2021
Décision du 24 décembre 2021

CONCLUSIONS

M. Laurent Domingo, rapporteur public

Vous avez à connaître de plusieurs recours dirigés contre trois décrets du 2 décembre 2020 (n°s 2020-1510, 2020-1511, 2020-1512) modifiant les dispositions du code de la sécurité intérieure relatives aux traitements de données à caractère personnel dénommés respectivement « Enquêtes administratives liées à la sécurité publique » (EASP), « Prévention des atteintes à la sécurité publique » (PASP) et « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP)[1].

Ces trois traitements de données, nés sur les cendres de l'éphémère et controversé fichier Edvige (décret n°2008-632 du 27 juin 2008 retiré par le décret n° 2008-1999 du 19 novembre 2008), ont été créés par des décrets du 16 octobre 2009 pour les deux premiers (décret n° 2009-1250 pour EASP ; décret n° 2009-1249 pour PASP) et un décret du 29 mars 2011 pour le troisième, pris après le rattachement de la Gendarmerie nationale au ministère de l'intérieur (décret n° 2011-340). Vous avez statué sur les recours dirigés contre ces décrets par des décisions du 11 mars 2013[2].

Si ce n'est pas la première fois que les textes régissant ces fichiers, aujourd'hui codifiés dans le code de la sécurité intérieure (respectivement aux articles R. 236-1 et s. pour EASP, R. 236-11 et s. pour PAPS et R. 236-21 et s. pour GIPASP)[3], font l'objet de modifications, celles résultant des décrets en litige du 2 décembre 2020 sont significatives : elles ont non seulement eu pour objet de mettre le cadre juridique applicable à ces fichiers en conformité avec la loi du 6 janvier 1978 modifiée en conséquence de l'adoption du RGPD[4] et de la directive « police-

[1] Des demandes en référé de suspension de l'exécution de ces décrets ont été rejetées par des ordonnances du 4 janvier 2021, n° 447970, n° 447972, n° 447974.
[2] Syndicat de la magistrature et autres, n° 334188 ; Association SOS Racisme Touche pas à mon pote et Syndicat de la magistrature et autres, n°s 332886, 334189 ; Association SOS Racisme Touche pas à mon pote, n° 348613
[3] Décret n° 2013-1113 du 4 décembre 2013 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du code de la sécurité intérieure.
[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces

justice »[5] et de régulariser certaines pratiques dans l'utilisation de ces traitements[6], mais aussi de faire officiellement entrer ces fichiers dans le champ de la sûreté de l'Etat, ce qui en fait donc, désormais, des fichiers mixtes, relevant tout à la fois du titre III et du titre IV de la loi de 1978. Il en a donc résulté une refonte significative des dispositions réglementaires applicables, même si, comme nous allons le voir, certaines sont demeurées inchangées.

Rappelons, pour commencer, les finalités de ces trois fichiers :

EASP a pour finalité de faciliter la réalisation d'enquêtes administratives, préalables à des décisions administratives prises en matière d'emplois, d'accès à des installations, de naturalisation, de délivrance de titres ou de décorations[7], par la conservation des données issues de ces enquêtes et dans la perspective de futures enquêtes relatives à la même personne (art. R. 236-1). Ce n'est donc pas un traitement constitué en vue de réaliser des enquêtes administratives, qui le sont avec le traitement Accred[8], mais en vue de traiter et conserver les données issues de ces enquêtes.

PASP (pour la DGPN) et GIPASP (pour la DGGN) ont pour finalité de recueillir, de conserver et d'analyser les informations qui concernent 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 (articles R. 236-11 et R. 236-21). Sont tout autant concernées des activités terroristes par exemple que des actions de violence collective, en particulier en milieu urbain ou à l'occasion de manifestations sportives.

Le ministre de l'intérieur indique en défense qu'EASP comprend 222 000 fiches, tandis que PASP en comporte 60 000 et GIPASP quelques 67 000.

I. Quelques moyens des quinze recours portent sur la compétence et la régularité, et nous commencerons par eux.

---

données, et abrogeant la directive 95/46/CE.

[5] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

[6] Délibérations de la CNIL du 25 juin 2020, n° 2020-064, n° 2020-065 et n° 2020-066.

[7] Enquêtes effectuées pour vérifier, préalablement aux décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation sur divers emplois publics ou privés, que le comportement des personnes intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées ; celles effectuées pour s'assurer, avant d'autoriser l'accès d'une personne autre que spectatrice ou participante, à tout ou partie des établissements et installations accueillant des grands événements exposés, par leur ampleur ou leurs circonstances particulières, à un risque exceptionnel de menace terroriste, que le comportement ou les agissements de cette personne ne sont pas de nature à porter atteinte à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'Etat ; et aussi celles effectuées dans le cadre des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux.

[8] Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD).

A. D'abord, la Collectivité territoriale de Corse et les 54 élus de l'Assemblée de Corse co-requérants (qui avaient soulevé sur ce point des QPC qui n'ont pas été renvoyées[9]) soutiennent que les trois décrets en litige sont entachés d'incompétence, parce que seule une loi pouvait les autoriser, au motif qu'en permettant le traitement de données concernant des élus locaux et des collectivités locales, ils affectent le principe de libre administration des collectivités locales.

Il faut toutefois rappeler qu'en vertu de l'article 34 de la Constitution (et de son Titre XII), ainsi que de la jurisprudence du Conseil constitutionnel, la loi fixe les règles concernant le régime électoral des assemblées locales ainsi que les conditions d'exercice des mandats électoraux et des fonctions électives des membres des assemblées délibérantes des collectivités territoriales et détermine les principes fondamentaux de la libre administration des collectivités territoriales, de leurs compétences et de leurs ressources. Relèvent ainsi de la loi les règles relatives à l'organisation, au fonctionnement et aux attributions des collectivités territoriales, qui doivent assurer l'effectivité de leur libre administration.

Or, le simple fait de traiter des données concernant des collectivités territoriales ou des élus locaux, dès lors qu'elles le sont pour des finalités légitimes, en l'espèce portant sur la réalisation d'enquêtes administratives ou la prévention des atteintes à la sécurité publique ou à la sûreté de l'Etat, ne saurait affecter le principe de la libre administration des collectivités territoriales, en ce compris les conditions d'exercice des mandats électoraux et des fonctions électives : en particulier, l'organisation, le fonctionnement, les compétences de la collectivité territoriale ne sont pas en cause ; les moyens dont disposent les élus pour accomplir leur mandat ou leur fonction sont inchangés.

Les requérants corses insistent plus particulièrement sur le traitement des opinions politiques. Mais, il faut d'abord relever que, sur ce point, les collectivités territoriales ne sont alors pas concernées : comme toute personne morale, elles ont une personnalité juridique, un patrimoine, des droits et libertés, mais on ne peut y inclure celle d'avoir des opinions politiques, car une personne morale n'a pas de conscience indépendante de celle des organes qui la représentent. Elle peut prendre des actes qui ont une signification politique, une portée politique, mais nous ne sommes pas dans le champ de la liberté de conscience et d'opinion. S'agissant des élus, s'ils font valoir la « menace d'une surveillance » de leurs activités « au travers d'un traitement arbitraire de leurs données personnelles par le pouvoir central », tout risque peut être écarté, eu égard aux finalités des traitements en cause. Les élus locaux, dont les élus Corses, sont des élus de la République qui n'ont ainsi pas vocation, en cette qualité, à être qualifiés de personnes physiques dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou à la sûreté de l'Etat. Et qu'ils le seraient, que leur enregistrement dans PASP et GIPAPS serait alors justifié, indépendamment de leur statut d'élu local, qui ne confère aucune sorte d'immunité.

Le moyen d'incompétence peut donc être écarté ainsi que, pour les mêmes motifs, les mêmes moyens soulevés sur le fond.

---

[9] 10 JS, 22 juillet 2021, n°s 449461, 449468, 449469.

Sur cette question d'incompétence du pouvoir réglementaire, la Quadrature du Net s'est subitement avisée de soulever à son tour une QPC, identique dans ses trois recours, cette fois contre les I et II de l'article 31 de la loi du 6 janvier 1978. Le I prévoit que les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui intéressent la sûreté de l'Etat, la défense, la sécurité publique ou le domaine police-justice sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la CNIL. Cette disposition a déjà été déclarée conforme à la Constitution (décision n° 2004-499 DC du 29 juillet 2004), sans qu'un changement de circonstances ne soit intervenu depuis. En outre, les traitements en litige ont été autorisés par des décrets, si bien que le I n'est au surplus pas applicable au litige.

Le II prévoit que ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6, c'est-à-dire, des données sensibles, sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la CNIL. Pour LQDN, comme les traitements de données personnelles mettent en cause les droits et libertés, en particulier lorsque sont traitées des données sensibles, l'article 31 a méconnu l'article 34 de la Constitution, selon lequel la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques, en reportant sur le pouvoir réglementaire le soin de fixer des règles dont la détermination n'a été confiée par la Constitution qu'à la loi. Comme si la loi du 6 janvier 1978, qui comporte les règles et garanties applicables aux traitements de données personnelles, n'existait plus et que le législateur devait donc lui-même autoriser tout traitement de données personnelles.

Le législateur peut créer des traitements de données. Il le fait d'ailleurs, renvoyant généralement à un acte réglementaire pour les modalités d'application. Le niveau législatif peut au demeurant être requis, en fonction en particulier de la technique de collecte envisagée et son caractère potentiellement intrusif pour la vie privée. Signalons d'ailleurs que la loi de 1978 l'envisage explicitement en matière de « police-justice » (articles 88 et 89). Mais, d'une part, l'article 31 de la loi de 1978 ne fait aucunement obstacle à l'intervention du législateur. La matière n'est pas réservée au règlement du fait de cet article 31. D'autre part, que la loi ou le décret autorise un traitement de données personnelles, les garanties de la loi de 1978 s'appliquent, sauf à ce que le législateur y déroge, ce que ne peut faire en revanche le règlement. Dans ces conditions, le moyen soulevé n'est manifestement pas sérieux, et il n'y a donc pas lieu de renvoyer au Conseil constitutionnel cette QPC de dernière minute.

B. Sur la procédure, la Quadrature du Net soutient, pour EASP seulement, que le décret le concernant est intervenu au terme d'une procédure irrégulière faute d'avoir été précédé d'une analyse d'impact. Son moyen est fondé sur les dispositions de l'article 62 de la loi du 6 janvier 1978 et celles de l'article 27 de la directive police-justice, ce qui est inopérant : l'article 62 de la loi de 1978 est relatif aux traitements de données du Titre II relevant du RGPD, ce qui n'est pas le cas d'EASP ; et l'article 27 de la directive police-justice a été transposé à l'article 90 de la loi de 1978, c'est-à-dire dans son Titre III.

Vous pourrez toutefois redresser le moyen et vous placer d'office sur le terrain de cet article 90, ce qui vous conduira à préciser qu'à la différence de l'analyse d'impact de l'article 62, qui doit être effectuée préalablement à la mise en œuvre du traitement et non nécessairement

avant l'adoption du texte qui l'autorise, l'analyse d'impact de l'article 90 doit, lorsque le traitement est mis en œuvre pour le compte de l'Etat, être adressée à la CNIL saisie pour avis, ce qui implique que l'analyse d'impact précède le texte autorisant le traitement : autrement dit, si le moyen tiré de la méconnaissance de l'article 62 de la loi de 1978 est, s'agissant des traitements relevant du titre II, inopérant (v. 6 novembre 2019, Fédération des acteurs de la solidarité et autres, n°s 434376, 434377, B), il est, s'agissant des traitements mis en œuvre pour le compte de l'Etat relevant du Titre III et donc de l'article 90, opérant. En l'espèce, il manque cependant en fait, l'analyse d'impact ayant bien été élaborée et transmise à la CNIL.

C. Plusieurs requêtes soutiennent que la CNIL a été, s'agissant des traitements PASP et GIPASP, irrégulièrement consultée, car, entre les projets de texte qui lui ont été soumis et les décrets publiés sont intervenues des modifications significatives sur lesquelles elle ne s'est pas prononcée. En la matière, votre jurisprudence, rappelée en particulier par Ass. 23 octobre 1998, Union des fédérations CFDT des fonctions publiques et assimilés (UFFA- CFDT), n° 169797, p. 360 (v. aussi par ex. 11 mars 2013, Syndicat de la magistrature et autres, préc. ; 29 janvier 2018, Société Marineland, société Safari Africain de Port St Père et autre, n°s 412210 412256, A) s'attache à vérifier si l'organisme consulté a rendu son avis en étant saisi de l'ensemble des questions soulevées par le texte, ce qui implique qu'il doit être à nouveau consulté si, après avoir rendu son avis, le gouvernement envisage d'apporter au texte des modifications qui posent des questions nouvelles.

C.1 La première modification en débat porte sur la possibilité de mettre en œuvre, dans les fichiers PASP et GIPASP, des techniques d'utilisation d'un gabarit biométrique pour la reconnaissance faciale à partir de la photographie[10]. Mais la CNIL s'est bien prononcée sur ce point, en indiquant justement que si tel devait être le cas (et ça ne l'est pas dans les décrets, raison d'ailleurs pour laquelle il n'y a pas eu d'étude d'impact à ce sujet), elle devrait être saisie d'une modification par voie réglementaire.

C.2 La seconde modification concerne le champ des données sensibles. Par principe, le traitement de ces données est interdit, sauf dérogation (article 6). En vertu de l'article 88 de la loi du 6 janvier 1978, le traitement de données sensibles est possible dans le domaine « police-justice » si, notamment, il est autorisé par une disposition législative ou réglementaire. C'est à cette fin que les décrets du 2 décembre 2020 concernant PASP et GIPASP, après avoir confirmé le principe de l'interdiction, ont modifié les exceptions à ce principe, et en particulier ont remplacé les « activités politiques, philosophiques, religieuses ou syndicales » par « des opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale ».

Le ministre reconnaît que la CNIL n'a pas été saisie de ces modifications[11], mais il soutient qu'il ne faut y voir qu'une question purement rédactionnelle, qui ne changerait rien sur le fond. Il explique, en substance, que les catégories de données qui peuvent être collectées,

[10] Dans EASP, le « traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie ».
[11] La CNIL l'a indiqué dans un communiqué du 11 décembre 2020 « Publication des décrets relatifs aux fichiers PASP, GIPASP et EASP : la CNIL précise sa mission d'accompagnement ».

traitées et conservées sont fixées aux articles R. 236-12 (PASP) et R. 236-22 (GIPASP) et les articles R. 236-13 et R. 236-23 ne font qu'autoriser, au sein de ces catégories, le traitement de certaines données sensibles. Pour le ministre, comme les données traitées ne portent que sur des activités, lorsque les décrets permettent que soit traitées des données relatives aux opinions politiques, aux convictions philosophiques ou religieuses ou à une appartenance syndicale, il ne peut s'agir que de données en réalité restreintes à des activités politiques, philosophiques, religieuses ou syndicales. Autrement dit, rien n'a changé, les articles R. 236-13 et R. 236-23 ne faisant que reprendre l'énoncé de l'article 6 de la loi de 1978, qui envisage les opinions et convictions ou l'appartenance, et non les activités.

On ne peut qu'adhérer au premier temps du raisonnement. Les articles qui autorisent le traitement de données sensibles n'ajoutent pas à la liste des données énumérées par les articles qui précèdent ; les données sensibles autorisées sont inclues dans la liste des données du traitement[12].

En revanche, le deuxième temps du raisonnement ne peut être retenu : dans les listes des données pouvant figurer dans le traitement, il y a en effet des activités, mais aussi des données qui peuvent être identifiées comme se rattachant à une opinion ou une conviction.

En particulier, si les 5° des I des articles R. 236-12 et R. 236-22 s'intitulent « Activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'Etat », tout ce qui y figure n'implique pas que les données pouvant être collectées se limitent à des « activités ». En matière politique, philosophique, religieuse ou syndicale, de telles activités, c'est par ex. se rendre à un meeting politique, c'est fréquenter tel lieu de culte ou célébrer une fête religieuse, c'est participer à telle manifestation organisée par un syndicat : autant d'exemples qui sont évidemment tout à fait insuffisants pour donner lieu à un traitement dans les fichiers PASP ou GIPASP, puisqu'encore faut-il que cette fréquentation, cette célébration ou cette participation puisse être considérée comme des données susceptibles de révéler une atteinte à la sécurité publique ou à la sûreté de l'Etat, mais si tel devait être le cas ils relèveraient bien du a) activités publiques ou au sein de groupements ou de personnes morales ou du f) sur la pratique religieuse.

Cependant, ce 5° prévoit aussi le traitement des données relatives aux comportements et habitudes de vie (b), aux activités sur les réseaux sociaux (d) ou au comportement religieux (f) (auquel on peut ajouter les « éléments ou signes de radicalisation » du 6°) : ce n'est plus seulement d'activités dont il est question, mais possiblement d'opinions, de convictions ou d'appartenance. Si par ex., sur n'importe quel réseau social, une personne explique à d'autres qu'elle se retrouve dans l'idéologie de tel groupuscule extrémiste, qu'elle cautionne et qu'elle soutient, ce n'est pas une activité politique, mais une opinion politique. Dans l'ancienne version du texte, cette information, qui est une donnée sensible, ne pouvait être traitée. Dans la nouvelle version, elle peut l'être.

---

[12] Ce qui est tout à fait évident avec les 1° et 3° des articles R. 236-13 et R. 236-23, les « signes physiques particuliers et objectifs comme éléments de signalement des personnes » renvoyant au f) du 1° du I des articles R. 236-12 et R. 236-22 et les « données de santé révélant une dangerosité particulière » renvoyant au c du 6° du I des mêmes articles.

Sauf sur un point, nous y reviendrons, nous sommes d'avis que ce n'est pas illégitime, mais là n'est pas encore la question. A ce stade, il s'agit de savoir si c'est à tort que la CNIL n'en a pas été saisie. C'est le cas, car, entre une activité et une opinion, il y a bien une différence de nature qui fait qu'entre le texte soumis à la CNIL et le texte publié, une question nouvelle, relative au champ des données sensibles collectables, est apparue. Rappelons d'ailleurs que lorsque la CNIL s'était prononcée, en 2009 et 2010, sur les décrets d'origine de PASP et GIPASP, elle n'avait pas manqué de relever « avec intérêt » que la notion d'« activités », notion objective[13] car fondée sur des actes, avait été substituée à celle, plus subjective, d'« opinions » politiques, philosophiques, religieuses ou syndicales, qui figurait dans le fichier Edvige.

Nous vous proposons donc d'annuler les nouveaux 2° des articles R. 236-13 et R. 236-23 du CSI, c'est-à-dire les 2° des articles 3 des décrets PASP et GIPASP du 2 décembre 2020.

D. Pour en terminer sur ces questions de régularité, vous pourrez constater que le ministre a justifié de ce que les décrets ne comportent pas de dispositions qui différeraient à la fois du projet initial du Gouvernement et du texte adopté par la section de l'intérieur du Conseil d'Etat.

[13] Dans la décision du 11 mars 2013 sur le décret PASP (n°s 332886, 334189 préc.), ces données relatives à des « activités » sont considérées comme de « nature factuelle et objective ».

II. Examinons maintenant les moyens de légalité interne soulevés par les requêtes, qui sont souvent communs aux trois fichiers, mais parfois aussi propres à EASP d'un côté et PASP/GIPASP de l'autre.

Nous vous proposons de procéder en retenant un ordre correspondant pour l'essentiel aux dispositions régissant ces fichiers et aux moyens soulevés en abordant successivement : les finalités ; les personnes concernées ; les données traitées ; les données sensibles ; les données relatives aux mineurs ; les rapprochements entre fichiers ; la durée de conservation des données ; l'accès aux données ; enfin, la sécurité des fichiers[14].

Une remarque liminaire : les décrets du 2 décembre 2020 sont des décrets modificatifs et ce n'est, par principe, qu'en tant qu'ils modifient le code de la sécurité intérieure qu'ils peuvent être contestés par les présents recours. Si les décrets ne disent rien ou s'ils ne font que confirmer des dispositions existantes (sans tirer les conséquences d'une nouvelle législation v. 7 décembre 2018, Société TBF Génie Tissulaire, n° 410887, aux tables), les requérants ne peuvent alors utilement soulever des moyens qui mettent en réalité en cause des dispositions figurant déjà dans le code de la sécurité intérieure. Il convient cependant, à notre sens, d'apporter un tempérament à ce principe, s'agissant de traitements de données qui répondent à des séries d'exigences liées les unes aux autres, en particulier liées aux finalités du traitement et aux données collectées, lorsque les modifications résultant du décret attaqué peuvent avoir, au moins dans cette mesure, des incidences sur la légalité des dispositions existantes, le décret modificatif pouvant alors être critiqué en tant qu'il n'a pas prévu des modifications supplémentaires qui s'imposaient. C'est dans cette perspective que nous aborderons les questions soulevées par les requêtes, en cantonnant les possibles inopérances aux seuls cas où les décrets attaqués ne sont aucunement en cause.

A. Sur les finalités

La finalité d'EASP n'a pas changé. EASP sert toujours à conserver les données issues de précédentes enquêtes administratives pour les besoins de futures enquêtes administratives. Ce qui est nouveau, c'est que, officiellement maintenant, parmi les données figurant dans le fichier, il en est qui relèvent de la sûreté de l'Etat, parce que les services, dès lors que des enquêtes administratives ont aussi un tel objet, peuvent collecter une information sur une personne intéressant la sûreté de l'Etat.

De leur côté, PASP et GIPASP servent toujours à recueillir, conserver et analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou, dorénavant, ce qui ne fait que régulariser la pratique[15], à la sûreté de l'Etat. Les finalités de PASP et GIPASP ont ainsi évolué, dans les textes du moins.

[14] Aucun moyen n'est soulevé contre les articles relatifs aux droits des personnes (R. 236-9, R. 238-19 et R. 239-29).
[15] v. Délibérations CNIL n°s 2020-064 et 2020-065, préc.

Par des moyens diversement argumentés, les requêtes soutiennent que les finalités des trois fichiers ne seraient pas suffisamment déterminées, explicites et légitimes (article 4 de la loi du 6 janvier 1978). Vous vous êtes déjà prononcées, dans vos décisions du 11 mars 2013 précitées sur les finalités des fichiers, mais est ici plus particulièrement en cause la sûreté de l'Etat.

Vous pourrez écarter les moyens qui reprochent aux décrets de décembre 2020 d'être insuffisamment précis en se référant à la notion de sûreté de l'Etat : ils ont pris le soin de préciser que 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, sachant que les intérêts fondamentaux de la Nation sont définis à l'article L. 811-3 du CSI (v. aussi art. 410-1 du code pénal) et que le Conseil constitutionnel a déjà jugé qu'il s'agit d'une notion habituellement utilisée par le législateur et appliquées par le juge, qui n'est entachée d'aucune imprécision (décision n° 2018-773 DC du 20 décembre 2018, Loi relative à la lutte contre la manipulation de l'information). En outre, les décrets attaqués ont pris soin de préciser, pour tenir compte d'une observation de la CNIL, que ces données intéressant la sûreté de l'Etat font l'objet, de façon isolée ou groupée, d'une identification dans le traitement.

Vous pourrez aussi écarter les moyens qui mettent en cause la légitimité de l'utilisation d'EASP, PASP et GIPASP pour les besoins de la sûreté de l'Etat, non pas en tant que l'utilisation d'un traitement de données personnelles pour assurer la préservation de la sûreté de l'Etat ne serait pas légitime – car elle l'est assurément – mais au motif qu'il existe déjà des fichiers concernant la sûreté de l'Etat, et il en existe d'ailleurs déjà plusieurs. Même si dans votre récente décision Médecins du monde et autres du 24 septembre 2021 (n° 441317) vous n'avez pas glissé un « en tout état de cause » en répondant à un moyen similaire concernant le système de contrôle automatisé, nous pensons que ce moyen est inopérant : ce n'est pas parce que d'autres services collectent des informations versées dans un fichier qui intéresse également la sûreté de l'Etat, et qui répond à des règles qui lui sont propres, qu'il est illégitime qu'un autre fichier puisse avoir aussi comme finalité de traiter des données participant à la sûreté de l'Etat. Les droits des individus nous semblent d'autant mieux garantis que leurs données sont traitées dans des fichiers distincts et, si ce n'est cloisonnés, du moins dont les liens possibles sont encadrés plutôt que dans un gigantesque fichier unique créé pour répondre à tous les besoins de tous les services concourant à la sûreté de l'Etat.

B. Sur les personnes concernées

Vous devrez écarter la critique formulée par plusieurs requêtes selon laquelle, avec l'ajout de la sûreté de l'Etat, les champs personnels des fichiers se seraient considérablement élargis, la LDH soutenant même que ces fichiers sont susceptibles « de concerner la quasi-totalité de la population française » ou la CTC estimant qu'ils peuvent couvrir « potentiellement l'intégralité de la population française ». De manière générale, qu'un fichier concerne un nombre important de personnes n'est pas en soi une cause d'illégalité, dès lors que les personnes concernées répondent aux finalités légitimes du fichier[16].

[16] Selon le ministre en défense, TAJ comprend 18,9 millions de fiches en 2019.

En outre, en l'espèce, pour EASP, la critique est avant tout inopérante, car les enquêtes administratives concernées par EASP sont toujours les mêmes, le décret du 3 décembre 2020 ne comportant aucune disposition nouvelle sur ce point. D'ailleurs, la critique ne concerne en réalité pas EASP lui-même, mais la définition du champ des enquêtes administratives. En tout état de cause, les enquêtes administratives visées par EASP sont loin de concerner la presque totalité de la population française car ne sont concernées par EASP que celles des personnes faisant l'objet d'une enquête administrative, au motif qu'elles font l'objet d'une décision administrative, positive ou négative, en matière d'emploi, d'accès à des installations, de naturalisation, de délivrance de titres ou encore de décorations, et il y a donc nécessairement une adéquation entre les personnes relevant d'EASP et le champ de ces enquêtes administratives.

Par ailleurs, si EASP prévoit que peuvent être enregistrées comme données des personnes physiques celles relatives à leurs activités publiques ou au sein de groupements ou de personnes morales, il n'est pas prévu que ces personnes morales ou ces groupements puissent eux-mêmes faire l'objet d'un enregistrement distinct dans le traitement. Elles ne peuvent l'être qu'à raison de l'activité de la personne physique, et cette information ne peut être recherchée automatiquement (dernier alinéa du R. 236-2).

Pour PASP et GIPASP en revanche, sont visées, dès les articles R. 236-11 et R. 236-21 du CSI, les informations qui concernent les personnes physiques ou morales ou les groupements, c'est-à-dire les groupements de fait sans personnalité juridique. Dans la mesure où ce n'est qu'à raison d'une activité individuelle ou collective indiquant que ces personnes physiques ou morales ou ces groupements peuvent porter atteinte à la sécurité publique ou à la sûreté de l'Etat qu'elles peuvent voir leurs données inscrites dans PASP et GIPASP, le champ personnel du traitement est, nécessairement, correctement délimité au regard de sa finalité.

Vous aurez remarqué cependant que les articles sur les données (R. 236-12 et R. 236-22) ne visent que des données de personnes physiques, tant aux I, qu'aux II, III et IV, ce qui s'explique par la circonstance que la loi du 6 janvier 1978 (comme le RGPD et la directive police-justice) ne s'applique qu'aux données des personnes physiques. Les décrets en litige ne disent rien des données des personnes morales, et ce n'est pas critiqué dans les requêtes.

Ce qui est critiqué, ce sont les personnes visées aux II, III et IV, c'est-à-dire l'entourage (qui figurait déjà dans les dispositions antérieures) et les victimes. Cette définition du champ personnel des deux traitements est toutefois strictement encadrée. L'entourage, ce sont les personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne fichée. Les décrets citent notamment les parents et les enfants. Mais ils ne seront pas systématiquement mentionnés. Et d'autres personnes peuvent l'être. Mais elles ne pourront l'être que dans la mesure où les données les concernant sont légalement collectées, ce qui signifie que les dispositions critiquées n'ont pas pour objet et ne peuvent avoir pour effet de méconnaître, par exemple, le secret médical ou le secret des relations avec l'avocat. Quant à la notion de victime, elle est suffisamment compréhensible.

Ensuite, ces tiers ne font pas l'objet d'une fiche séparée, mais des données les concernant peuvent être enregistrées dans la fiche de la personne principale. Surtout, les finalités de cet enregistrement sont limitées : dans la stricte mesure où ces données sont nécessaires pour le suivi de la personne principale ; dans la stricte mesure où ces données sont nécessaires à la protection des intérêts de la victime et à la prévention de la réitération de faits par la personne principale (dans un sens similaire, propre à la finalité de ce fichier, v. 27 mai 2021, M..., n° 441977, à propos du « système d'information sur les armes »). En outre, les données en cause sont également restreintes à l'identification, aux coordonnées, à la situation et aux activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'Etat, sauf les déplacements. Aucune donnée sensible ne peut être collectée à ce titre.

S'agissant de ces tiers, un seul point nous interroge, mais il ne met pas en cause la légalité des décrets. En réponse à une demande d'information, le ministre vous a indiqué que dans PASP les données des tiers ne pouvaient pas être recherchées par le traitement, mais que c'était en revanche possible dans GIPASP (en dépit de la similitude des textes, l'architecture de l'interface de ces deux traitements diffère assez sensiblement). Dès lors que la finalité des fichiers ne porte que sur les informations des personnes principales, nous ne sommes pas certains de la régularité de telles recherches. Mais c'est une question d'application, pas une question de texte.

C. Sur les données traitées

Les données d'un traitement doivent être notamment adéquates, pertinentes et, pour les traitements relevant des titres III et IV, non excessives.

Aussi bien pour EASP que pour PASP et GIPASP, la liste des données susceptibles d'être enregistrées est longue, particulièrement longue, surtout si on la compare avec l'état du droit antérieur. Certains requérants en font d'ailleurs un moyen d'illégalité : l'augmentation considérable du nombre des items figurant aux nouveau articles R. 236-2, R. 236-12 et R. 236-22 serait une preuve de ce que les données collectées sont excessives. Mais ce n'est cependant pas, en soi, une cause d'illégalité. Au contraire, là où les anciens textes comportaient des entrées générales, comme « activités publiques, comportement et déplacements », que vous aviez validées dans vos décisions de mars 2013, les décrets en litige ont entendu, pour chaque catégorie de données, préciser ce qu'elles recouvraient et donc, aussi, ce qu'elles ne recouvrent pas, afin précisément d'éviter au mieux de collecter des données inadéquates en pratique.

Dans cette optique, de manière générale, les données dont le traitement est autorisé par les décrets de décembre 2020 ont été définies avec précision, si bien que, généralement, la critique tirée de l'indétermination ou du caractère excessif de telle ou telle donnée doit être écartée. En effet, il ne faut pas omettre de lire la liste des données en tenant compte des limites qui sont fixées, pour chaque catégorie de données avec la finalité poursuivie par le traitement et pour chaque entrée au regard de sa catégorie : rappelons que les articles R. 236-2, R. 236-12 et R. 236-22 autorisent l'enregistrement de données dans la stricte mesure où elles sont nécessaires à la poursuite d'une finalité du traitement et que les données

mentionnées ne peuvent être traitées que si elles relèvent effectivement de la catégorie à laquelle elles appartiennent.

Un seul exemple, mais la réponse est la même pour nombre d'autres cas évoqués dans les requêtes : les « comportement et habitudes de vie » ou « déplacements » ou encore « pratiques sportives », qui relèvent du 5°, ne peuvent être enregistrés que dans la mesure où, c'est le titre de ce 5°, il s'agit d'activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'Etat. Autrement dit, contrairement à ce que soutient le CNB par ex., qu'une personne, au titre d'un comportement ou d'une habitude de vie, préfère le thé ou le café, n'a aucune raison de se retrouver dans les fichiers.

Dans ces conditions, le risque invoqué de fichage généralisé de la population doit être écarté, non seulement parce que, comme nous vous l'avons dit, toute la population n'est pas concernée, mais aussi parce que toutes les données des personnes concernées ne sont pas visées, sauf bien sûr mésusage des fichiers, ie usage illégal des fichiers. Mais les décrets attaqués ont au contraire pour objet de fixer les frontières de la légalité des données.

Restent néanmoins certains items en particulier, qui peuvent prêter à discussion.

1. « Activités sur les réseaux sociaux », au titre du 5° (donc en tant qu'il s'agirait d'une activité susceptible de porter atteinte à la sécurité publique ou à la sûreté de l'Etat). Trois questions au moins se posent.

Quels réseaux sociaux ? La notion juridique de « réseaux sociaux » n'existe pas et les décrets attaqués n'en fournissent pas. Le code de la consommation (article L. 111-7, auquel il n'est en tout état de cause pas renvoyé) se réfère aux services de communication au public proposés par les opérateurs de plateforme en ligne, lesquels comprennent notamment « la mise en relation de plusieurs parties en vue (…) de l'échange ou du partage d'un contenu (…) », ce qui est assez proche, mais sans les recouvrir exactement (cf. un réseau peer-to-peer par ex.), des réseaux sociaux.

Le ministre, en défense, estime que les réseaux sociaux sont « toute plateforme ouverte susceptible de refléter l'activité numérique d'une personne », ce qui est à peu près la définition d'un site internet. Pourquoi, alors, ne pas avoir écrit « activité numérique » ? Inversement, pourquoi avoir ciblé spécifiquement les « réseaux sociaux », alors qu'en tout état de cause, l'activité numérique d'une personne peut être traitée au titre de son « activité publique » ou de ses « comportements » ? A ce titre d'ailleurs, si vous deviez annuler l'entrée « activités sur les réseaux sociaux », vos décisions n'auraient pas de conséquence sur la faculté dont disposent les services de police et de gendarmerie compétents pour traiter, au titre du 5°, des données d'origine numérique.

Partant de ce constat, nous sommes d'avis qu'en dépit, en l'état du droit positif, de l'imprécision du terme « réseaux sociaux », votre décision aura plus d'effet utile en validant, après avoir apporté les précisions nécessaires, cette entrée qu'en l'annulant purement et simplement. En vous inspirant par ex. de la définition du projet de règlement DMA selon lequel un « service de réseaux sociaux en ligne » est « une plateforme permettant aux

utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations »[17], vous pourrez considérer qu'un réseau social (en ligne) est une plateforme permettant à des utilisateurs d'échanger des contenus et d'interagir. Vous pourrez alors préciser ce qu'il faut entendre par « activités » et la manière dont les données résultant de cette activité peuvent être collectées.

Quelles activités ? Il va de soi, mais il ne sera pas inopportun de le dire, que les décrets en litige n'ont pas autorisé le « piratage » des réseaux sociaux et que ce n'est donc, en principe (car sous réserve du recours à des techniques de renseignement par les services habilités), que l'activité « publique », ie visible et accessible, sur les réseaux sociaux, dépendant des paramètres du réseau et des réglages de l'utilisateur, qui peut être traitée. Les 3° permettent d'ailleurs l'enregistrement des identifiants utilisés (entendus comme les pseudonymes, sites ou réseaux concernés, autres identifiants techniques), à l'exclusion des mots de passe. En outre ne peuvent être traitées que les données de l'utilisateur ; les données personnelles des tiers (par ex. par un « retweet ») ne peuvent y être inclues, sauf si l'activité sur les réseaux sociaux (ou numérique de manière générale) conduit à identifier une personne physique entretenant ou ayant entretenu des relations directes et non fortuites avec la personne physique ou morale pouvant porter atteinte à la sécurité publique ou la sûreté de l'Etat (hypothèse des II et IV).

Quelle collecte ? Dans ses avis, la CNIL considérait que les décrets devraient exclure explicitement la possibilité d'une collecte automatisée de ces données. Les décrets attaqués ne le font pas, mais on ne peut aucunement y voir une autorisation de le faire : la collecte automatisée de données en ligne, par un logiciel fonctionnant sur le base d'un algorithme, constitue un traitement de données différent de ceux autorisés par les trois décrets en litige et il ne pourrait donc être mis en œuvre qu'après avoir été explicitement autorisé. Le silence des décrets ne vaut donc pas autorisation.

2. « Données relatives aux troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur », au titre des facteurs de dangerosité (6°).

Les 3 décrets autorisent la collecte de ces données et, comme il s'agit de données de santé, on les retrouve (sous une formulation différente mais équivalente) dans les articles sur les données sensibles. Vous pourrez considérer qu'il s'agit, contrairement à ce que soutiennent les requérants, de données adéquates et pertinentes, en relevant que ne sont pas visés des diagnostics établis par un professionnel de santé, mais des données qui portent sur des comportements, observables, qui ont une origine psychologique ou psychiatrique et qui révèlent une dangerosité (et non une fragilité au sens du 7°). Et à ce titre, le secret médical n'est pas remis en cause car au contraire, précisément, ces données ne peuvent être collectées que conformément aux dispositions législatives et réglementaires en vigueur, c'est-à-dire que le secret médical énoncé à l'article L. 1110-4 du code de la santé publique fait obstacle à ce

[17] 7) de l'article 2 du projet de règlement relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques).

que les données en cause soient obtenues auprès des professionnels intervenant dans le système de santé, soumis à ce secret.

3. « Antécédents judiciaires (nature des faits et date) » et « suites judiciaires », toujours comme des facteurs de dangerosité (6°).

Ces données sont mises en cause par les requêtes au regard de l'article 777-3 du code de procédure pénale, selon lequel (alinéa 2) : « 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 ».

Mais comme la CNIL l'a rappelé dans ses avis, les décrets en litige, qui n'en avaient nullement la capacité, n'ont pas entendu déroger à cette règle législative si bien que les fichiers EASP, PASP et GIPASP peuvent comporter des données d'antécédents judiciaires ou de suites judiciaires, mais sans mention d'un jugement ou d'un arrêt de condamnation.

En outre, encore une fois, des données relatives aux antécédents judiciaires et aux suites judiciaires ne peuvent figurer dans les fichiers qu'à raison, car ils sont prévus dans cette catégorie, d'un facteur de dangerosité et qu'au regard de la finalité poursuivie par le traitement.

D. Sur les données sensibles

Dans le fichier EASP, était déjà autorisé l'enregistrement de données, contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des fonctions ou des missions envisagées alors même que ce comportement aurait une motivation politique, religieuse, philosophique ou syndicale et il a été ajouté, aussi, le comportement qui tiendrait à la dangerosité que feraient apparaitre les données, obtenues conformément aux dispositions législatives et réglementaires en vigueur, relatives aux troubles psychologiques ou psychiatriques de l'intéressé.

Dans les fichiers PASP et GIPASP, les signes physiques particuliers et objectifs comme éléments de signalement des personnes ont été conservés ; les activités politiques, philosophiques, religieuses ou syndicales ont été remplacées par les opinions politiques, les convictions philosophiques ou religieuses ou une appartenance syndicale ; et ont été ajoutées les données de santé révélant une dangerosité particulière.

1. En premier lieu, une question générale doit être posée (même si en toute rigueur, elle n'est opérante que pour les dispositions nouvelles) en ce qui concerne la justification de la nécessité de traiter de telles données.

De quelle nécessité parle-t-on ? Dans le champ du titre III, l'article 88, reprenant l'article 10 de la directive « police-justice », rend possible le traitement de données sensibles uniquement en cas de nécessité absolue[18]. Mais dans le champ du titre IV, aucune condition particulière de

nécessité n'est prévue. Ce n'est pas pour autant que vous ne pouvez pas exercer un contrôle de nécessité, bien au contraire, car la possibilité de traiter des données sensibles doit être justifiée. Mais le législateur n'ayant pas entendu qualifier particulièrement la nécessité d'y recourir, vous pourrez vous en tenir à un contrôle d'adéquation simple entre le traitement de ces données et la finalité « sûreté de l'Etat » du fichier.

Cela étant dit, il s'agit bien d'une exigence de fond et non d'une condition formelle : les décrets autorisant le traitement de données sensibles n'ont pas besoin de rappeler qu'ils l'autorisent parce qu'il est nécessaire ; mais la nécessité doit bien être vérifiée.

2. Justement, en deuxième lieu, sont discutées les nouvelles catégories de données sensibles autorisées.

Nous vous avons proposé d'annuler les 2° dans les fichiers PASP et GIPASP pour un motif de régularité. Quelques mots sur le fond cependant. Les opinions politiques et les convictions philosophiques et religieuses nous apparaissent être des données nécessaires, et absolument nécessaires, au regard de la finalité des fichiers (cf. 11 juillet 2018, Ligue des droits de l'homme, n° 414827 pour le fichier ACCReD). Car un discours extrémiste, radicalisé, dangereux demeure, aussi, de l'ordre de l'opinion politique ou de la conviction philosophique ou religieuse. Le traitement de cette donnée dans les fichiers est justifié.

Nous ne sommes en revanche pas convaincus, dans les fichiers PASP et GIPASP[19], du caractère nécessaire et légitime des données sur l'appartenance syndicale. Les fichiers PASP et GIPASP ont pour objet de collecter des données qui intéressent les atteintes à la sécurité publique ou à la sûreté de l'Etat.

Or, par nature, appartenir à un syndicat, et même avoir une activité syndicale, ne constitue pas, et ne peut constituer, une cause d'atteinte à la sécurité publique ou à la sûreté de l'Etat. Les syndicats professionnels (ce sont eux qui sont concernés au titre des données sensibles) ont, en vertu du code du travail (article L. 2131-1), « exclusivement pour objet l'étude et la défense des droits ainsi que des intérêts matériels et moraux, tant collectifs qu'individuels, des personnes mentionnées dans leurs statuts ». Autrement dit, l'appartenance syndicale (comme, normalement, l'activité syndicale) ne peut être qu'en rapport avec cet objet ; elle est donc nécessairement légale. A défaut, on sort du champ syndical. Dit clairement, appartenir à la CGT (c'est la CGT qui soulève le moyen) n'est pas illégal et ne peut constituer une atteinte à la sécurité publique ou à la sûreté de l'Etat. S'il peut apparaître légitime, au regard de la finalité des traitements, de renseigner les activités publiques d'une personne ou ses activités au sein de groupements ou de personnes morales, y compris à l'occasion d'une activité syndicale identifiée et qui aurait, ça arrive, conduit à des comportements susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'Etat, nous n'identifions pas une même nécessité s'agissant de la seule appartenance syndicale.

---

[18] Laquelle nécessité se distingue de celle, sans qualificatif, résultant du RGPD mais que la jurisprudence de la Cour (se prononçant sur les dispositions identiques de la directive 95/46, au sujet du référencement des pages web) interprète comme étant « strictement nécessaire » (CJUE, 24 septembre 2019, C-136/17).

[19] EASP ne vise que des comportements qui auraient une motivation syndicale.

Alors certes, comme nous vous l'avons dit, les données sensibles autorisées ne s'ajoutent pas aux données traitées, elles sont comprises dans les données traitées, lesquelles portent en particulier sur des activités ou des opinions susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'Etat ou des facteurs de dangerosité, si bien qu'en pratique l'appartenance syndicale ne peut donc s'y trouver, de sorte que sa mention dans les décrets PASP et GIPASP est plus inutile qu'illégale. Et puisqu'il s'agit aussi de prévenir de mauvais usages des fichiers, cette mention est inopportune. En tout état de cause, nous proposons l'annulation pour un motif de procédure. Ce motif d'annulation, rapporté à l'intérêt particulier qui s'attache à l'utilisation de ces données pour la prévention des atteintes à la sécurité publique et à la sûreté de l'Etat, au moins en tant qu'elles portent sur des opinions politiques ou de convictions philosophiques ou religieuses, justifie que leur suppression ne s'impose qu'à partir d'un délai permettant au gouvernement, s'il le souhaite, de prendre une mesure réglementaire autorisant régulièrement leur collecte (v. 19 juillet 2010, Fristot et Mme Charpy, n° 334014, B sur ce point).

Quant aux 3° sur les données de santé révélant une dangerosité particulière, il ne s'agit que des données relatives aux troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur. Pour les raisons déjà indiquées, autoriser le traitement de ces données répond aussi à une nécessité, et une nécessité absolue, au regard des finalités des fichiers en litige.

3. Il convient enfin de relever que, dans les trois décrets, il est interdit de procéder à des recherches automatisées ou de sélectionner une catégorie particulière de personnes sur la base des données sensibles[20], ce qui constitue une des garanties appropriées pour les droits et libertés de la personne concernée au sens de l'article 88 de la loi du 6 janvier 1978 (en ce sens 27 mai 2021, M. M..., n° 441977, à propos du « système d'information sur les armes »).

E. Sur les données relatives aux mineurs

Dans vos décisions du 11 mars 2013 préc., vous avez déjà validé l'application des décrets EASP et PASP aux mineurs. En particulier, pour PASP (et on peut en dire de même pour GIPASP), vous avez jugé qu'aucune stipulation conventionnelle, notamment pas celles des articles 3-1 et 16 de la convention internationale relative aux droits de l'enfant, ni aucune disposition législative ou réglementaire ni aucun principe ne fait obstacle à ce que soit autorisé l'enregistrement, dans un traitement automatisé, de données relatives à des mineurs[21] et vous avez contrôlé que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée réponde à des finalités légitimes et que le choix, la collecte et le traitement des données soient effectués de manière adéquate et proportionnée au regard de ces finalités.

[20] R. 236-13 et -23 dans PASP et GIPASP, article R. 236-2 in fine pour EASP.
[21] Dans le même sens, v. 21 septembre 2015, Association de défense et d'assistance juridique des intérêts des supporters et autres, n°s 389815 et a., à propos du fichier STADE ; 13 avril 2021, Ligue des droits de l'Homme et autres, n°s 439360 et a., à propos de GendNotes

Avec les décrets attaqués, les dispositions relatives aux mineurs n'ont pas été modifiées. Si la sûreté de l'Etat a été ajoutée et si le champ des données collectées a été détaillé, il n'apparaît cependant pas que l'application des décrets EASP, PASP et GIPASP aux mineurs soient pour autant, dorénavant, entachée d'illégalité.

D'une part, des mineurs âgés de seize ans au moins peuvent toujours, dans certains cas, faire l'objet d'une enquête administrative. Leurs données, collectées conformément aux règles des articles R. 236-1 et s., peuvent figurer dans EASP eu égard à la finalité limitée de ce fichier.

D'autre part, des mineurs âgés d'au moins treize ans étant susceptibles de porter atteinte à la sécurité publique et, le cas échéant, à la sûreté de l'Etat, ils peuvent donc figurer dans PAPS et GIPAPS, sachant qu'eu égard à la finalité de ces fichiers, des garanties spécifiques existent, s'agissant de la durée de conservation des données, réduite, ou de l'intervention d'un référent national spécialement créé pour assurer le respect des garanties accordées aux mineurs.

F. Sur les rapprochements entre fichiers

Il faut indiquer qu'il n'y a pas d'interconnexion entre les fichiers, c'est-à-dire de mise en relation automatique entre les fichiers, de « branchements » des uns ou autres si l'on peut dire, mais seulement des rapprochements autorisés avec certains fichiers, c'est-à-dire des mises en relations « manuelles » qui consistent à consulter, directement ou indirectement, un fichier pour renseigner une information dans un autre fichier. Les moyens des requêtes fondés sur l'interconnexion sont donc inopérants.

Il faut également indiquer que les rapprochements envisagés, tant pour EASP, PASP et GIPASP, consistent, d'une part, en l'indication, qui est une information en soi, de l'enregistrement ou non de la personne dans d'autres traitements de données à caractère personnel, dont la liste est limitativement énumérée (TAJ, N-SIS II, FPR, FSPRT, FOVeS et EASP, PASP et GIPASP eux-mêmes, v. 8° de l'article R. 236-2 et 8° des I des articles R. 236-12 et R. 236-22), mais aussi, d'autre part, en la consultation d'autres fichiers, directement ou indirectement selon les règles de ces autres fichiers, pour renseigner une des autres données autorisées par les décrets (par ex. la donnée « armes et titres afférents » peut conduire à utiliser les données contenues dans les fichiers sur les armes). Les données en cause étant légitimes au regard des finalités des trois fichiers en litige, et limitées par ces finalités, les rapprochements en cause sont justifiés. Les moyens qui postulent la disproportion de ces données au seul motif qu'elles ont été collectées à l'occasion d'un traitement créé pour une autre finalité doivent donc être écartés.

Ajoutons aussi que, contrairement à ce que soutiennent plusieurs requêtes, les décrets en litige n'autorisent pas, ni même n'envisagent ou dissimuleraient la possibilité pour une personne accédant directement à EASP, PASP ou GIPASP de pouvoir en conséquence, consulter, en direct et librement, l'intégralité des autres fichiers dans lesquels ces données figurent. Les articles, dans les décrets en litige comme dans ceux des autres fichiers, relatifs aux données, aux accès directs ou indirects et à l'enregistrement des opérations, constituent le cadre qui, justement, ouvrent et ferment les portes entre les fichiers, dans le but de séparer les données contenues dans les fichiers relevant de ministères, de services ou de personnels différents.

G. Sur la durée de conservation des données

Les durées de conservation des données n'ont pas été modifiées : il s'agit toujours de 5 ans pour EASP et 10 ans pour PAPS et GIPASP (mais 3 ans pour les mineurs). Si en revanche les dispositions relatives aux données collectées ont fait l'objet de modifications, elles ne nous apparaissent pas, et à plus forte raison pour la sûreté de l'Etat, devoir remettre en cause ce que vous aviez jugé en 2013, à savoir que les durées de conservation n'excédent pas la durée nécessaire pour répondre aux finalités des traitements, sachant que chacun des trois textes ne prévoient pas que les données sont impérativement conservées cinq ou dix ans, mais qu'elles peuvent être conservées au maximum 5 ans (EASP) ou au plus 10 ans (PASP et GIPASP ; 3 ans pour les mineurs).

H. Sur l'accès aux données

Classiquement, dans les fichiers EASP, PASP et GIPASP, le code de la sécurité intérieure distingue entre ceux qui peuvent accéder directement aux données, par consultation du fichier, et ceux qui peuvent accéder indirectement aux données, par leur transmission après une demande.

Des moyens sont soulevés contre les règles relatives à l'accès à EASP, mais ces règles n'ont été que très marginalement modifiées, et ce n'est que dans cette mesure que les moyens sont opérants. Le décret de décembre 2020 concernant EASP a ajouté, dans les accédants directs, les services du renseignement territorial des directions territoriales de la police nationale à ceux des directions départementales de la sécurité publique, car en Guyane, à Mayotte et en Nouvelle-Calédonie, il y a des DTPN et non des DDSP[22], et il a remplacé le terme de « fonctionnaire » par « agent », car, de fait, il n'y a pas seulement des fonctionnaires dans les services chargés du renseignement, mais aussi des contractuels. Ce n'est pas le lieu de s'interroger sur cette évolution de notre fonction publique, et il convient seulement de relever que ce sont des agents des mêmes services de renseignement et qu'ils sont également individuellement désignés et spécialement habilités, si bien que les garanties relatives aux conditions d'accès à EASP demeurent inchangées.

Des moyens sont également soulevés en ce qui concerne PASP et GIPASP, et ils ne sont opérants, cette fois, qu'en ce qui concerne les règles relatives aux accédants indirects figurant aux III des articles R. 236-26 et R. 236-36, car ce sont ces dispositions qui ont fait l'objet de véritables modifications par les décrets de décembre 2020[23]. Il est soutenu que les destinataires des données seraient trop largement définis.

Selon les III nouveaux, peuvent être destinataires des données, dans la limite du besoin d'en connaître :

---

[22] Décret n° 2019-1475 du 27 décembre 2019 portant création et organisation des directions territoriales de la police nationale.

[23] Pour l'accès direct : dans PASP, on retrouve aussi l'ajout de la DTPN ; dans GIPASP, une série d'enquêtes administratives existantes est ajoutée.

1° Les personnes ayant autorité sur les services ou unités accédant aux données directement ou indirectement en vue de la réalisation d'enquêtes administratives. Ce qui, concrètement, vise les supérieurs hiérarchiques de ces services, tels que le ministre de l'intérieur, le DGPN ou le DGGN, les préfets ou encore les directeurs départementaux de la sécurité publique. Il est légitime que ces autorités, lorsqu'elles doivent prendre des décisions, puissent solliciter, dans la limite du besoin d'en connaître, une information figurant, selon les cas, dans PASP ou GIPASP.

2° Les procureurs de la République : ce n'est pas contesté en soi et leur reconnaître un accès indirect aux informations n'est en effet pas illégitime.

3° et 4° : les agents du renseignement de la PN, de la GN ou d'un service spécialisé et les personnels de la PN ou les militaires de GN qui ne sont pas chargés d'une mission de renseignement. Ce sont ces dispositions qui concentrent les critiques des requêtes. Mais, en réalité, c'était déjà la règle existante puisque pouvaient accéder indirectement aux informations des fichiers « tout autre agent d'une unité de la gendarmerie nationale ou d'un service de la police nationale ». Ce qui change c'est que dans le cercle du renseignement, il y a désormais une autorisation individuelle du supérieur hiérarchique ; ce n'est qu'en dehors du renseignement que l'agrément des demandes a été conservé. Cette seule modification de procédure, qui ne marque pas un recul des garanties mais une simplification des procédures, n'affecte pas la détermination des destinataires, qui sont les mêmes et, il faut le rappeler, qui ne peuvent être des destinataires que pour le besoin de connaître de l'information demandée, c'est-à-dire pour l'exercice de leurs fonctions et lorsque l'information demandée est nécessaire. Tout autre usage de l'accès indirect aux fichiers constituerait une illégalité.

Dans votre décision du 11 mars 2013 sur le fichier PASP (n° 332886, préc.), vous avez souligné que la possibilité d'accéder au traitement « dans la limite du besoin d'en connaître »[24] est suffisamment encadrée dès lors qu'elle renvoie ainsi aux finalités du traitement. C'est-à-dire que « le verrou du « besoin d'en connaître » exclut tout accès de confort ou de curiosité » (conclusions A. Lallet sur votre décision rendue à propos du fichier GendNotes, 13 avril 2021, LDH et autres, n° 439360), sachant que comme les autres opérations, celles de consultation, de communication et de transfert des données 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 (R. 236-27 et R. 236-37).

I. Sécurité

Sont enfin soulevés des moyens qui mettent en cause la fiabilité technique des fichiers. Mais si les responsables de traitement ont des obligations en la matière, ce n'est pas un sujet qui relèvent de l'autorisation de traiter des données mais du seul fonctionnement des traitements

[24] On trouve parfois la formule « dans la stricte limite du besoin d'en connaître » et les précisions « à raison de leurs attributions et dans la stricte limite où l'exercice de leurs compétences le rend nécessaire » (fichier GendNotes par ex.), ce qui constitue autant de précautions rédactionnelles, mais ne nous semble pas impliquer un degré de garanties supplémentaires par rapport à la seule formule du « besoin d'en connaître ».

en cause (v. vos décisions précitées du 11 mars 2013 ; 11 avril 2014, Ligue des droits de l'homme, n°s 352473, 352527 ; 13 avril 2021, Ligue des droits de l'homme, n° 439960 ; 24 septembre 2021, Médecins du monde et autres, n° 441317).

PCMNC :
- au non renvoi des QPC ;
- au rejet des requêtes dirigées contre le décret n° 2020-1510 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » ;
- à l'annulation des 2° des articles 3 des décrets n° 2020-1511 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique » et 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 » ;
- à ce que l'Etat verse à, respectivement, la CGT et autres co-requérants, l'association La Quadrature du Net, et le Conseil national des barreaux, une somme de 1500 euros chacun au titre des frais d'instance ;
- au rejet du surplus des conclusions.