**431350 – Association CRPA**
**431530 – Ligue des droits de l'homme**
**432306 – MGEN Action sanitaire et sociale**
**432329 – Association Avocats, droits et psychiatrie**
**432378 – Conseil national de l'ordre des médecins**
**435722 - Syndicat des psychiatres des hôpitaux**

**10ème et 9ème chambres réunies**

**Séance du 13 mars 2020**
**Lecture du 27 mars 2020**

# CONCLUSIONS

## M. Alexandre Lallet, rapporteur public

Ni la médecine, ni les sciences humaines et sociales n'ont encore éclairci de façon satisfaisante les liens entre radicalisation à caractère terroriste et troubles psychiatriques. S'il existe un consensus sur le fait que la radicalisation n'est pas en elle-même une maladie mentale, les études peinent à identifier si et dans quelle mesure une telle pathologie peut constituer un facteur causal ou prédisposant, ou la conséquence d'un processus d'endoctrinement ou de dérive extrémiste. L'incertitude scientifique nourrit logiquement la polémique, qui trouve aujourd'hui un espace d'expression juridique.

Vous vous souvenez sans doute du fichier HOPSYWEB, créé par un décret du 23 mai 2018[1] que vous avez annulé très partiellement par une décision inédite du 4 octobre 2019 (Association CRPA et autres, n° 421329, 422497 et 424818). Il s'agit d'un traitement de données à caractère personnel réalisé à l'échelle départementale, placé sous la responsabilité de chaque agence régionale de santé, dont la finalité première est d'assurer le suivi administratif des personnes faisant l'objet de soins psychiatriques sans consentement[2].

Dès sa création, il a été reproché à l'administration d'avoir privilégié la logique sécuritaire sur l'approche sanitaire. Il est peu dire que le décret attaqué donne du crédit à cette critique. Mettant en œuvre la mesure n° 39 du plan national de prévention de la radicalisation du 23 février 2018, ce décret n° 2019-412 du 6 mai 2019 assigne à HOPSYWEB une nouvelle finalité, consistant à informer le préfet de l'admission en soins psychiatriques sans

[1] Décret n° 2018-383
[2] S'y ajoute, depuis l'origine, une finalité statistique, ainsi que celle d'informer le préfet sur un éventuel séjour en établissement psychiatrique d'une personne sollicitant un permis de détention d'armes soumises à autorisation.

consentement des personnes afin de prévenir la radicalisation à caractère terroriste. Le nouvel article 2-1 du décret de 2018 permet désormais, pour cette seule finalité, de mettre en relation les noms, prénoms et dates de naissance des personnes figurant dans ce traitement avec le fichier des signalements pour la prévention de la radicalisation à caractère terroriste, le FSPRT, et précise que, lorsque ce croisement de données révèle une correspondance, le préfet du département où les soins ont été délivrés et, le cas échéant, les agents qu'il désigne à cette fin, en sont informés. L'objectif affiché est d'identifier, parmi les personnes signalées dans le FSPRT, celles qui sont susceptibles de présenter, en raison d'une pathologie mentale, des risques accrus d'atteinte à la sûreté des personnes ou à l'ordre public et d'améliorer leur surveillance et leur suivi.

L'avis critique de la CNIL sur le projet de décret décrit le fonctionnement concret de cette mise en relation et ses suites[3] : dès l'inscription d'une nouvelle personne dans l'un ou l'autre fichier et toutes les 24 heures au moins, un croisement des données « noms », « prénoms » et « dates de naissance » de chacun des fichiers est réalisé. En cas de concordance, le FSPRT génère un mail à destination du préfet du département d'hospitalisation et des agents qu'il a habilités pour les en informer. Ces derniers peuvent contacter l'ARS afin de s'assurer de l'identité de la personne concernée dans le cadre d'une procédure dite de « levée de doute » et d'obtenir des informations complémentaires portant sur les dates de début et de fin de la mesure, le type de mesure prononcée ou encore le lieu d'hospitalisation. Ces démarches aval[4] ne sont toutefois pas mentionnées dans le décret.

---

[3] Elle la qualifie d'interconnexion/ Cette qualification, qui est sans incidence dans le présent litige, n'a rien d'évidente au regard de la jurisprudence, dont il faut bien admettre qu'elle ne brille pas par sa clarté. Une interconnexion doit être regardée comme l'objet même d'un traitement qui permet d'accéder à, d'exploiter, et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu. La mise en relation de fichiers qui se limite à des données dont le recueil a été déclaré pour chacun d'eux et qui n'élargit pas le champ de collecte de l'un ou de l'autre de ces traitements automatisés ne constitue pas une interconnexion (CE, 19 juillet 2010, *F... et C...*, n° 317182-323441, au Rec.). L'interconnexion est ainsi un sous-ensemble des « mises en relation », qui ne recouvre, comme l'indiquait Julien Boucher dans ses conclusions sur cette affaire, que les mises en relation « occultes », consistant à étendre indirectement le périmètre des données traitées dans le « fichier de destination ». En l'occurrence, nous n'avons pas trouvé trace d'une modification du décret créant le FSPRT pour prévoir l'exploitation de données issues d'HOPSYWEB. On pourrait donc considérer que le recueil de ces données n'a pas été « déclaré » pour chacun d'eux, au sens de cette jurisprudence, et que nous sommes bien en présence d'une interconnexion, du point de vue du FSPRT.

[4] Cette procédure de levée de doute soulève deux interrogations. La première est juridique : aucun texte ne prévoit l'utilisation de ces données complémentaires aux fins de prévenir la radicalisation terroriste. La seconde est opérationnelle. Nous ne voyons pas bien l'utilité de la procédure de « levée de doute » alors que le préfet est censé disposer en propre de ces informations complémentaires, soit parce qu'il est l'auteur de la mesure sur le fondement des articles L. 3213-1 et suivants du code de la santé publique, soit parce que l'article L. 3212-5 du même code fait obligation au directeur d'établissement qui prononce l'admission du patient à la demande d'un tiers ou en cas de péril imminent d'en informer sans délai le préfet, soit encore parce que les admissions en soins psychiatriques ordonnées par le juge pénal sur le fondement de l'article 706-135 du code de procédure pénale sont immédiatement portées à la connaissance du préfet en vertu de ce texte. Par ailleurs, dès lors que le décret attaqué prévoit l'information du préfet du lieu d'hospitalisation, il ne s'agit pas de données relatives à des patients hospitalisés dans d'autres départements. Au fond, c'est davantage la nature de la pathologie qui pourrait être intéressante dans la perspective du croisement avec le FSPRT, mais HOPSYWEB – qui n'est pas un fichier médical - ne la contient pas. Nous ne sommes d'ailleurs pas certain que le préfet puisse en disposer, alors que

*

Le passage des six requêtes dont vous êtes saisis au tamis de la recevabilité fera quelques victimes :

- les conclusions de l'association « Avocats, droits et psychiatrie » dirigées contre le décret du 23 mai 2018 sont tardives[5] ;

- la requête du Conseil national de l'ordre des médecins (n° 432378) est irrecevable. Comme vous l'avez jugé le 4 octobre dernier, ce dernier n'a intérêt pour agir qu'en tant que les intérêts des médecins sont en cause. Or contrairement au décret de 2018, le décret de 2019 ne porte que sur les données d'identification des patients. Il en va de même de la requête du syndicat des psychiatres des hôpitaux (n° 435722) ;

- enfin, nous pensons que la requête de la MGEN Action sanitaire et sociale est également irrecevable. Cette mutuelle se prévaut de sa qualité de gestionnaire d'établissements de santé prenant en charge des personnes faisant l'objet de soins psychiatriques sans consentement, en reprochant au décret de dénaturer leurs missions de santé publique en y ajoutant une activité de police. Mais tel n'est évidemment pas la portée de ce texte. Les établissements n'interviennent à aucun moment dans le traitement résultant du décret attaqué. Les données traitées ne portent que sur les patients, et non sur les établissements.

  Aucune disposition du code de la santé publique ne confère aux établissements de santé la mission de représenter leurs patients. Ils n'ont donc pas à s'en faire les porte-paroles dans le prétoire, pas plus qu'ils ne sont « propriétaires » des données qu'ils versent dans HOPSYWEB et qui sont ensuite utilisées selon les finalités prévues par le décret. La contestation de la MGEN est d'ordre politique et moral.

  En tout état de cause, vous pourrez rejeter au fond cette requête.

*

---

l'article L. 3212-5 du code de la santé publique a été modifié par l'article 69 de la loi n° 2016-41 du 26 janvier 2016 pour supprimer la communication au préfet des certificats médicaux et du bulletin d'entrée du patient admis sur décision de l'établissement.

[5] Précisons qu'en revanche, l'intérêt pour agir de cette association, que vous aviez admise dans votre décision d'octobre dernier, n'est pas douteux car elle s'est donnée pour objet de défendre les clients faisant l'objet de mesures de soins sans consentement, et non les intérêts de la profession d'avocat. Dans ce dernier cas, une association ne justifie pas d'un intérêt à demander l'annulation d'un acte dont les dispositions ne concernent pas, en tant que tels, les membres de la profession d'avocat, alors même qu'elles peuvent affecter la situation de certains clients (CE, 23 mars 2005, *Institut des avocats conseils fiscaux*, n° 264997, au Rec.).

**Avant d'en arriver là, il vous faudra d'abord déterminer le cadre juridique applicable**. C'est la question la plus délicate que pose ce dossier.

Rappelons que les traitements de données à caractère personnel se répartissent à cet égard en trois catégories :

- la généralité d'entre eux est soumise au RGPD, tel que précisé et complété, le cas échéant, par les dispositions de la loi du 6 janvier 1978 ;
- les traitements 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* », relèvent de la directive dite « police-justice » du 27 avril 2016[6] et des dispositions de la loi du 6 janvier 1978 qui la transposent ;
- enfin, les traitements qui ne relèvent pas du champ d'application du droit de l'Union, qui sont ceux intéressant la sûreté de l'Etat et la défense nationale, sont exclusivement soumis aux dispositions communes de la loi du 6 janvier 1978 et aux dispositions spécifiques figurant désormais aux articles 115 et suivants de cette loi.

La notion de « *sûreté de l'Etat* » est utilisée depuis l'origine par la loi du 6 janvier 1978, mais au sein du triptyque des « fichiers de souveraineté » comprenant aussi la défense nationale et la sécurité publique[7]. Vous vous êtes donc borné jusqu'à présent à ranger certains fichiers dans cette catégorie, sans définir les contours propres du sous-ensemble que constituent les fichiers de sûreté de l'Etat.

La sûreté de l'Etat est un vocable ancien du droit pénal que le code pénal de 1992 a remplacé par celui d'« *intérêts fondamentaux de la nation* », énumérés à l'article 410-1 et au nombre desquels figurent la sécurité de la nation et la sauvegarde de la population[8]. La ligne de partage précise avec la sécurité publique n'est pas absolument évidente à tracer. Il y a sans doute lieu de s'attacher à l'ampleur de la menace et aux objectifs poursuivis par ceux qui en sont à l'origine, qui doivent consister à porter atteinte aux institutions ou à la cohésion nationale[9], et non pas simplement affecter la sécurité du quotidien.

---

[6] 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.

[7] Ce triptyque recouvre les traitements dont l'acte de création peut ne pas être publié et à l'égard desquels le droit d'accès s'exerce en principe de manière indirecte.

[8] On peut en rapprocher le concept de « *sécurité nationale* » qui figure à l'article L. 1111-1 du code de la défense : « *La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter* ».

[9] Les fichiers intéressant la sûreté de l'Etat sont, au premier chef, les fichiers relevant de la politique de renseignement, qui vise à « *concourir à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation* » (art. L. 811-1 du code de la sécurité intérieure).

Selon les termes d'un récent rapport parlementaire, le FSPRT, dont l'acte de création n'a pas été publié[10], « *recense et centralise les informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités terroristes* »[11]. Il est placé depuis décembre dernier sous la responsabilité de la direction générale de la sécurité intérieure, c'est-à-dire l'un des services spécialisés de renseignement mentionnés à l'article R. 811-1 du code de la sécurité intérieure[12]. Il est en outre au nombre des traitements intéressant la sûreté de l'Etat énumérés à l'article R. 841-2 de ce code, dont le contrôle relève de la formation spécialisée du Conseil d'Etat. Nous pensons que cette qualification est exacte eu égard à l'objet de ce fichier et à la menace que les activités terroristes font peser sur la nation, quand bien même les infractions terroristes relèvent-elles d'un titre distinct de celui qui traite des atteintes aux intérêts fondamentaux de la nation.

Le traitement HOPSYWEB d'origine relève quant à lui du RGPD, à tout le moins en ce qui concerne sa finalité première de suivi des patients faisant l'objet de mesures de soins sans consentement[13].

**La difficulté tient au statut juridique de la mise en relation de deux traitements qui relèvent de cadres juridiques différents.**

Rappelons que le traitement de données à caractère personnel est défini, en droit de l'Union, auquel renvoie le droit national, comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel* ». Constituent notamment un traitement l'« extraction », le « rapprochement » ou encore « l'interconnexion ». De là, deux analyses sont possibles :

---

[10] Décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[11] Rapport d'information n° 1335 sur les fichiers mis à la disposition des forces de sécurité.

[12] Il était initialement géré par l'unité de coordination de la lutte antiterroriste rattachée à la direction générale de la police nationale.

[13] Nous pensons qu'il en va de même de la finalité consistant à informer le préfet d'une prise en charge psychiatrique sans consentement dans le cadre de l'instruction des demandes de détention d'armes. Certes, il s'agit d'un traitement réalisé à des fins de police administrative. Or la directive dite « police-justice » de 2016 couvre les traitements 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ». Mais son considérant 12 illustre cette dernière formule par les activités de police lors de manifestations, de grands évènements sportifs et d'émeutes, le maintien de l'ordre public nécessaire pour prévenir des infractions pénales et les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non. Nous ne pensons pas, par conséquent, que l'ensemble des activités de police administrative relèvent du champ de la directive police-justice. En particulier, l'instruction des demandes de détention d'armes nous paraît trop éloignée d'une éventuelle infraction pour justifier son application.

- soit, comme la CNIL l'a fait dans son avis, on considère que le décret attaqué n'ajoute qu'une opération nouvelle à un traitement qui serait constitué d'HOPSYWEB dans son ensemble, et on lui applique alors le régime juridique correspondant à la **finalité principale** de ce macro-traitement : à cette aune, il est évident que la mise en relation avec le FSPRT ne constitue qu'une fonction accessoire d'HOPSYWEB, dont la vocation première n'est pas modifiée. Le décret de 2019 devrait alors être confronté au RGPD ;

- soit, dans une approche plus analytique, on regarde ce croisement de données à caractère personnel et le dispositif d'information du préfet comme formant un **traitement à part entière** et on lui applique le régime juridique inhérent à sa finalité propre. En l'occurrence, cette finalité, telle qu'elle ressort du décret attaqué, ne se distingue pas de celle du FSPRT. Même si nous comprenons que, techniquement, les opérations qu'elle implique ne prennent pas cette forme, elle aboutit à un résultat analogue à un traitement qui collecterait les données d'identification des patients dans HOPSYWEB pour les verser dans le FSPRT afin d'enrichir le profil des personnes qui y figurent, en y ajoutant la rubrique « *fait ou a fait l'objet de soins psychiatriques sans consentement : OUI/NON* ». Cette mise en relation est totalement étrangère au suivi administratif des patients dans les établissements. Dans cette logique, ce nouveau traitement intéresserait la sûreté de l'Etat au même titre que le FSPRT. Le décret attaqué devrait alors être confronté aux dispositions de la loi du 6 janvier 1978 applicables à cette catégorie de traitements, et non au RGPD.

Il y a matière à hésitation et nous comprenons tout à fait le parti retenu par la CNIL. Mais notre conviction est que la seconde orientation est la bonne, pour plusieurs raisons :

- en premier lieu, le droit de la protection des données à caractère personnel érige le traitement en « unité de compte juridique » et fait dépendre le cadre juridique applicable de sa finalité. Un traitement ne se confond pas avec l'application informatique qui la gère, ni avec la notion de fichier, définie par la loi de 1978 comme « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* ». Plusieurs traitements distincts peuvent être réalisés à partir d'un même logiciel ou d'un même fichier. Sans doute la définition du traitement que nous avons rappelée implique-t-elle qu'un unique traitement puisse lui-même se composer d'un « ensemble d'opérations ». Mais outre qu'on peut voir dans ce pluriel une référence à la récurrence d'opérations réalisées à partir d'un même traitement, par opposition à une opération unique[14], il ne peut s'agir, à notre avis, que d'un **ensemble cohérent d'opérations techniques concourant à la même finalité**. En l'espèce, il nous paraît bien difficile de voir dans le rapprochement litigieux une simple opération technique de plus dans un traitement unique que serait HOPSYWEB,

[14] Le singulier utilisé par le RGPD implique aussi qu'une opération unique puisse constituer un traitement.

alors que, comme les requêtes le soutiennent, elle introduit une véritable rupture dans sa logique initiale et poursuit une finalité étrangère à la raison d'être originelle ;

- en deuxième lieu, les textes européens nous paraissent conforter cette approche. Le paragraphe 1 de l'article 9 de la directive « police-justice » relatif aux données personnelles traitées pour des finalités relevant, pour les unes, de cette directive et, pour les autres, du RGPD ou qui sont hors champ du droit de l'Union, explicité par son considérant 34, prescrit de raisonner finalité par finalité. Il en ressort ainsi que le transfert de données contenues dans un fichier relevant de la directive à un destinataire tiers relèvera du RGPD s'il est transmis à d'autres fins que celles prévues par la directive, s'il n'est pas purement et simplement exclu du champ du droit de l'Union bien entendu. C'est aussi ainsi que nous comprenons le considérant 19 du RGPD. Et c'est la logique retenue par l'avis rendu par l'Assemblée générale du Conseil d'Etat sur la réforme du droit de la protection des données personnelles faisant suite au RGPD, à propos des traitements qu'elle a qualifiés de « mixtes », qui sont ceux dont les finalités relèvent pour partie du RGPD, et pour partie du droit interne. L'avis[15] préconise une application distributive des textes, sous réserve qu'elle soit intellectuellement possible[16]. En l'occurrence, la mise en relation ajoutée par le décret de 2019 est parfaitement dissociable des autres opérations prévues dans HOPSYWEB depuis l'origine.

- en troisième lieu, l'objectif poursuivi aurait pu être atteint par un texte prévoyant la création d'un traitement collectant des données conservées dans le FSPRT et HOPSYWEB pour les croiser, sans modifier le décret de création de ce dernier[17]. Il n'y aurait alors eu aucune raison de s'attacher à la finalité principale d'HOPSYWEB.

- enfin, l'approche analytique, par finalité, permet un réglage plus fin des droits des personnes et des obligations du responsable de traitement qui nous paraît opportun[18], fût-ce au prix d'une plus grande complexité. En l'occurrence, par exemple, le

---

[15] Avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, n° 393836, 7 décembre 2017, pts. 44-48 : « *S'agissant des traitements relevant à la fois du champ de la directive et de celui du droit interne, dès lors que les données sur lesquelles la personne concernée demande à exercer ses droits ne peuvent être exclusivement rattachées à l'un ou l'autre de ces deux champs, les restrictions apportées à ces droits ne pourront excéder celles prévues par la directive* ».

[16] Tel n'était pas le cas, par exemple, du traitement en cause dans l'affaire *Association des américains accidentels* du 19 juillet 2019, à nos conclusions. Il s'agissait en effet des mêmes opérations qui concouraient, d'une part, à la mission d'assiette, de liquidation et de recouvrement de l'impôt et, d'autre part, à la recherche des infractions fiscales. L'Assemblée du contentieux s'est donc attachée, conformément à la jurisprudence européenne, à la finalité première du traitement, lequel se rattachait en l'occurrence à sa première mission.

[17] Il s'agirait alors d'une interconnexion, à nos yeux (V. la note n° 3).

[18] Il n'est toutefois pas absolument nécessaire puisque l'article 23 du RGPD permet d'apporter, à certaines conditions, des restrictions aux droits des personnes à l'égard des traitements régis par ce règlement, notamment pour des motifs de « sécurité nationale » et de « sécurité publique ». Mais encore faut-il que l'acte créant le traitement le prévoie, ce qui n'est pas le cas en l'espèce.

rattachement du traitement de mise en relation litigieux aux traitements intéressant la sûreté de l'Etat présente l'intérêt de le soumettre au droit d'accès indirect, et d'éviter que, par le truchement d'une demande de communication des données ayant donné lieu à un signalement au préfet dans ce cadre, la personne concernée soit informée de sa présence dans le FSPRT.

Cette analyse vaut pour les mises en relation consistant à servir la finalité d'un traitement B en rapprochant les données qui y sont conservées avec celles qui sont issues du traitement A. Elle devrait aussi s'appliquer en cas de mise en relation en vue de servir une finalité tierce, laquelle déterminerait alors le cadre juridique applicable. Elle ne préjuge pas de la position à tenir en présence d'une mise en relation « réciproque » qui servirait la ou les finalités des deux fichiers, question que vous pourrez réserver[19].

Pour ce qui nous concerne aujourd'hui, **nous pensons donc que le RGPD ne peut être utilement invoqué**. Nous vous proposons toutefois de faire reste de droit en examinant les moyens au regard des dispositions homologues de la loi du 6 janvier 1978 applicables aux traitements intéressant la sûreté de l'Etat, lorsqu'elles existent. Les requérants ne seront donc en rien lésés par ce recadrage juridique.

*

Venons-en à la légalité externe du décret.

Ce dernier n'ayant pas la portée qui lui est prêtée s'agissant du secret médical – nous y reviendrons brièvement au stade de la légalité interne – il n'est pas entaché **d'incompétence** à ce titre, ni à aucun autre d'ailleurs. Conformément au II de l'article 26 de la loi du 6 janvier 1978 alors applicable, c'est bien par décret en Conseil d'Etat qu'il fallait autoriser ce traitement intéressant la sûreté de l'Etat et portant sur des données de santé.

La règle dite du « tiers texte » à laquelle obéit la **consultation du Conseil d'Etat** n'a pas été méconnue.

Au titre de la légalité externe, la MGEN soutient enfin que la **consultation de la CNIL** a été irrégulière, faute pour elle de disposer d'une analyse d'impact complète. Dans son avis, la CNIL a en effet indiqué que « *l'absence d'information précise sur l'architecture et les*

[19] En toute rigueur, il conviendrait de dissocier deux traitements au sein d'une telle mise en relation : le traitement « A => B » (flux de données issues de A pour enrichir les données de B) et le traitement « B => A ». Le traitement « bénéficiaire » (B dans le premier cas, A dans le second) déterminerait le cadre applicable à chacun de ces deux traitements. Si cette mise en relation prend la forme de deux actes, l'un modifiant l'acte créateur de A (pour prévoir l'utilisation des données issues de B afin de servir la finalité de A), l'autre de B (pour prévoir l'utilisation des données issues de A afin de servir la finalité de B), il pourrait y avoir matière à annuler l'un mais pas l'autre. Si cette mise en relation procédait d'un acte unique, il pourrait y avoir matière à l'annuler partiellement pour ne laisser subsister que l'un des traitements. La complexité opérationnelle de cette construction mérite toutefois d'approfondir la réflexion.

*mesures retenues ne permettent pas d'évaluer la conformité du dispositif à l'exigence de sécurité prévue par les articles 5-1-f) et 32 du RGPD* ».

L'article 35 du RGPD prescrit la réalisation d'une telle analyse lorsqu'un type de traitement, en particulier par le recours à de 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 libertés des personnes physiques. Lorsque l'analyse d'impact révèle que ce risque reste élevé en l'absence de mesures d'atténuation, l'article 36 du règlement prescrit au responsable de traitement de consulter l'autorité de contrôle, c'est-à-dire la CNIL, en lui fournissant l'analyse d'impact et le descriptif des mesures et garanties prévues pour réduire le risque. L'autorité qui estime ces mesures insuffisantes pour assurer le respect du RGPD émet un avis et peut faire usage de ses pouvoirs de sanction.

Si vous estimez, comme nous, que le décret attaqué n'est pas régi par le droit de l'Union, le moyen est inopérant car la loi du 6 janvier 1978 ne comporte aucune obligation équivalente pour les traitements intéressant la sûreté de l'Etat.

Si, au contraire, vous estimez le RGPD applicable, ou si vous envisagez de surmotiver votre décision en vous plaçant fictivement dans ce cadre, en tout état de cause, nous vous proposons de retenir la même solution d'inopérance, par un autre raisonnement.

Sans doute, dans ce référentiel juridique, la mise en relation litigieuse appelait-elle la réalisation d'une analyse d'impact, ce qui a été le cas, d'ailleurs. Il s'agit de rapprocher deux fichiers aux finalités originelles clairement distinctes, qui comportent tous les deux des données présentant une particulière sensibilité. Il est vrai que le décret se borne à permettre l'identification des personnes figurant dans l'un et l'autre fichiers, sans autre détail sur leur santé, le processus de radicalisation dans lequel elles sont engagées ou d'autres éléments de leur vie privée. Mais ce rapprochement peut ensuite motiver des actions de surveillance potentiellement très intrusives. En outre, le FSPRT a une portée nationale et concernerait plus de 20 000 personnes ; si HOPSYWEB est structuré au niveau départemental, il s'agit d'un fichier déployé à l'échelle nationale qui recense l'ensemble des personnes faisant l'objet de soins sans consentement, soit près de 100 000 en 2018[20].

Vous avez déjà jugé que l'obligation de réaliser une telle analyse d'impact relève de la mise en œuvre du traitement, de sorte que son absence est sans incidence sur la légalité de l'acte autorisant sa création (CE, 6 novembre 2019, *Fédération des acteurs de la solidarité et autres*, n° 434376-434377, aux T.). Cette solution se justifie tant par les termes de la loi du 6 janvier 1978, qui prescrit la réalisation de l'analyse d'impact préalablement à la « mise en œuvre » du traitement, que par la logique du RGPD, qui est celle de la responsabilisation des responsables de traitement. Le RGPD supprime les formalités préalables à la création du traitement, au profit d'un contrôle *a posteriori*, assorti de sanctions au quantum démultiplié.

[20] Etant rappelé que la durée de conservation des données, que vous avez validée en octobre dernier, est comprise entre trois et quatre ans, ce qui amplifie les effets de la mise en relation.

Dans ses conclusions conforme sur cette décision, notre collègue Sophie Roussel n'excluait pas que le défaut – ou l'irrégularité – de la consultation de la CNIL sur la base d'une analyse d'impact, sur le fondement du paragraphe 1 de l'article 36 du RGPD, puisse en revanche avoir une incidence sur la légalité de l'acte définissant les caractéristiques du traitement.

Cette solution nous paraît certaine pour les fichiers relevant de la directive police-justice. Son article 28 prévoit la consultation de la CNIL « *préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer* ». C'est la raison pour laquelle le 2ème alinéa de l'article 90 de la loi du 6 janvier 1978 qui le transpose prévoit expressément que, pour les traitements mis en œuvre pour le compte de l'Etat et relevant de la directive, l'analyse d'impact est adressée à la CNIL dans le cadre de la demande d'avis sur le projet d'acte de création du traitement.

Tel n'est pas le cas pour les traitements relevant du RGPD. Le paragraphe 1 de l'article 36 ne situe pas dans le temps le moment de la consultation de l'autorité de contrôle sur la base de l'analyse d'impact. Mais, en cohérence avec l'obligation de réaliser l'analyse d'impact avant la mise en œuvre du traitement, son considérant 84 précise qu'elle doit l'être « *avant que le traitement n'ait lieu* », c'est-à-dire avant sa mise en service[21]. Dans ces conditions, et dès l'instant que l'absence d'analyse d'impact est sans incidence sur la légalité de l'acte réglementaire créant le traitement, parce que celle-ci intéresse sa mise en œuvre, c'est-à-dire qu'elle se situe en aval de cet acte, nous ne voyons pas comment on pourrait reprocher à l'Etat de ne pas l'avoir fournie à la CNIL à l'appui d'une consultation prévue par le droit interne et qui n'a pas le même objet, puisqu'elle porte, en amont, sur la légalité de cet acte de création. Il n'y a pas lieu d'y loger, de façon presque opportuniste, un point de contrôle de l'analyse d'impact qui aurait déjà, le cas échéant, été réalisée, et qui relève d'un cas de consultation distinct et d'une autre logique[22].

---

[21] Le paragraphe 4 du même article 36 fait bien obligation aux Etats membres de consulter l'autorité de contrôle « *dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement* ». Mais aucun lien n'est fait avec le paragraphe 1 et l'analyse d'impact. Il s'agit d'une obligation de consultation distincte, comparable à celle que prévoit le a) du 4° de l'article 8 de la loi de 1978 préalablement à tout projet de loi ou de décret qui détermine dans certaines de leurs caractéristiques essentielles, les conditions de création ou de mise en œuvre d'un traitement de données à caractère personnel ou d'une catégorie de traitements (CE, 20 juin 2018, Syndicat national des vétérinaires d'exercice libéral et autres, n° 408185-408192, aux T.) - à ceci près que son champ est circonscrit aux traitements reposant sur une base législative spécifique. Par ailleurs, le paragraphe 5 du même article 36 prévoit que « *nonobstant le paragraphe 1, le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci* (...) ». Nous comprenons là encore, à travers la formule « *nonobstant le paragraphe 1* », qu'il s'agit d'un cas de consultation distinct de celle qui porte sur l'analyse d'impact, et qui trouve sa déclinaison dans les dispositions de la loi de 1978 prévoyant l'avis voire l'autorisation de la CNIL préalablement à la création de certains traitements.

[22] En l'espèce, nous sommes d'autant plus convaincu de l'inopérance du moyen que le reproche que la CNIL a adressé à l'analyse d'impact porte sur les mesures de sécurité, dont on a dit qu'elles intéressaient elles aussi la mise en œuvre du traitement, et non son acte fondateur, qui ne comporte et n'a vocation à comporter aucune

C'est ce qui explique selon nous qu'aucune disposition de la loi du 6 janvier 1978[23] ou de son décret d'application[24], notamment celles qui énumèrent les informations et pièces qui doivent être fournies à la CNIL à l'appui d'une demande d'avis sur un projet d'arrêté ou de décret de création d'un traitement régi par le RGPD, ne mentionne l'analyse d'impact[25].

Vous pourriez donc juger que la consultation de la CNIL sur le projet d'acte créant un traitement, en application de l'article 31 ou de l'article 32 de la loi de 1978, ne peut être viciée par l'absence ou l'insuffisance d'analyse d'impact.

Les moyens de légalité interne ne nous retiendront qu'en raison de leur nombre.

A l'évidence, **l'exigence d'adéquation, de pertinence et de proportionnalité** qui résulte de l'article 6 de la loi de 1978 est respectée, tant en ce qui concerne la nature des données traitées, qui sont limitées à ce qui est nécessaire à l'identification des bi-appartenants, que les destinataires de celles-ci, à savoir les préfets et agents placés sous leur autorité, qui sont en charge de la prévention de la radicalisation terroriste. Et en dépit des incertitudes scientifiques que nous décrivions, la **légitimité de la finalité poursuivie** n'est pas discutable. Au-delà de l'intuition nourrie par l'actualité récurrente et son lot d'agressions émanant de déséquilibrés se réclamant d'Allah, de Nice à Villejuif en passant par Villeurbanne et Metz, l'Etat peut légitimement souhaiter prioriser ou adapter les modalités de surveillance et de prévention du passage à l'acte des radicalisés souffrant de troubles psychiatriques. Si les chiffres les plus variables sont avancés selon les sources, un rapport d'information parlementaire de 2019 citant les déclarations du secrétaire d'Etat auprès du ministre de l'intérieur indique que 12 % des personnes enregistrées dans le FSPRT auraient un passé ou un présent psychiatrique.

---

disposition sur ce point. On peut certes imaginer, en théorie, que l'ampleur des mesures techniques ou organisationnelles de sécurisation à mettre en œuvre compte tenu de la sensibilité du traitement puisse interroger la pertinence même de le créer et dissuader l'Etat d'aller de l'avant. Mais outre que ce n'est certainement pas le cas ici, rien n'empêche l'Etat d'abroger l'acte de création du traitement au vu de ces considérations. Nous ne voyons donc pas comment les lacunes alléguées de l'analyse d'impact pourraient rejaillir sur la légalité du décret attaqué.

[23] V. article 30 de la loi ici applicable, et désormais article 33.

[24] Article 16 du décret n° 2005-1309 du 20 octobre 2005 (applicable en l'espèce) et, désormais, article 67 du décret n° 2019-536 du 29 mai 2019. L'article 110-1 du premier décret prévoyait la fourniture de l'analyse d'impact à l'appui de la demande d'avis sur les fichiers relevant de la directive police-justice. Désormais, le IV de l'article 130 du décret du 29 mai 2019 ne le prévoit que pour la consultation prévue au 3ème alinéa de l'article 90 de la loi du 6 janvier 1978 (traitements qui ne sont pas mis en œuvre pour le compte de l'Etat), et c'est le 2ème alinéa de cet article qui fait obligation à l'Etat de produire l'analyse d'impact à l'appui de la demande d'avis.

[25] Il est sans doute opportun qu'elle lui soit transmise lorsqu'elle a été réalisée, de même qu'il est souhaitable, comme le recommandent les lignes directrices du comité européen de la protection des données, que l'analyse d'impact soit lancée « *le plus tôt possible dans le cycle de conception du traitement* » (p. 17). C'est d'ailleurs un corollaire du principe « *privacy by design* » qui impose au responsable de traitement d'intégrer la problématique de la protection des données personnelles le plus en amont possible de ses projets. Mais aucun texte n'érige cette bonne pratique en obligation juridique, dont la méconnaissance pourrait affecter la légalité de l'acte de création du traitement.

Conformément au IV de l'article 8 de la loi de 1978, le **principe d'interdiction du traitement des données dites sensibles**, en l'occurrence des données de santé, n'est pas opposable aux traitements justifiés par l'intérêt public et autorisés par décret en Conseil d'Etat après avis publié et motivé de la CNIL, dans les conditions prévues au II de l'article 26[26]. Ces conditions sont remplies ici[27].

Contrairement à ce qui est soutenu, le décret, en tant qu'il prévoit une information du préfet, ne porte aucune atteinte au **secret médical** qui ne serait prévu par la loi[28]. Lorsqu'il n'est pas lui-même l'auteur de la mesure de soins psychiatriques sans consentement, le préfet en est informé sans délai par le directeur de l'établissement d'accueil ou par la juridiction qui a prononcé l'hospitalisation, en vertu du code de la santé publique. Le croisement des données d'HOPSYWEB avec celles du FSPRT ne fournit aucune information supplémentaire sur la santé de la personne. Il va de soi, naturellement, que les agents habilités placés sous la subordination du préfet bénéficient du même régime d'accès. En outre, comme on l'a dit, la procédure aval dite de « levée de doute » n'est pas régie par le décret attaqué, de sorte que le moyen tiré de ce que le préfet pourrait obtenir d'autres informations de l'ARS dans ce cadre, comme du reste tous les autres moyens de la Ligue des droits de l'homme critiquant cette procédure, sont inopérants[29].

Le décret attaqué ne méconnaît pas **l'article L. 3211-5 du code de la santé publique** dès lors que le croisement des données et l'information du préfet ne conduit pas à opposer aux personnes leurs antécédents psychiatriques dans la jouissance de leurs droits de citoyens.

Le décret litigieux n'affecte en rien les **missions des établissements et des professionnels de santé** telles qu'elles sont définies par le code de la santé publique.

Aucune disposition, notamment pas l'article 29 de la loi de 1978 alors applicable, ne prévoit que l'acte de création d'un traitement de données rappelle le **droit d'information** dont disposent les personnes concernées, dès l'instant qu'il n'est pas prévu d'y déroger[30].

---

[26] On peut se demander pourquoi le fichier HOPSYWEB d'origine a été autorisé par décret en Conseil d'Etat. La CNIL le justifiait par l'applicabilité de ce II de l'article 26 de la loi de 1978. Mais ce dernier, par la formule « *ceux de ces traitements...* », ne semble faire référence qu'aux traitements mentionnés au I, qui doivent remplir deux conditions : être mis en œuvre pour le compte de l'Etat et relever des finalités énumérées au 1° ou au 2°.

[27] Si le RGPD s'appliquait, il conviendrait de mobiliser l'exception prévue au g) du 2. de son article 9 (traitement « *nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* »).

[28] Le pouvoir réglementaire peut apporter au secret médical des restrictions prévues par la loi ou qui en sont la conséquence nécessaire (CE, 12 juin 1998, CNOM et autres, n° 183528 et a., aux T.).

[29] Précisons qu'il n'est pas soutenu que le décret dérogerait au secret médical en tant qu'il impliquerait la transmission d'informations au FSPRT, dont le responsable de traitement est la DGSI. Mais l'ensemble du processus est automatisé et crypté et nous comprenons qu'aucun agent de la DGSI n'est amené à prendre connaissance des données. C'est la raison pour laquelle la liste des destinataires des données ne les inclut pas.

[30] S'agissant d'un traitement intéressant la sûreté de l'Etat, une dérogation à l'obligation d'information est envisagée par le V de l'article 32 de la loi alors en vigueur. Mais dans ce cas, l'article 29 de la loi prescrit de le

Il ne peut être utilement reproché au décret de ne pas avoir prévu de mesures permettant de préserver **la sécurité des données** et de limiter le risque d'un accès par des tiers non autorisés, dès lors que les prescriptions que pose en la matière l'article 34 de la loi de 1978 intéressent la mise en œuvre du traitement et non la légalité de l'acte qui le crée (CE, 26 octobre 2011, *Association pour la promotion de l'image et autres*, n° 317827 et a., au Rec.)[31].

Il n'y a pas lieu d'annuler le décret attaqué **par voie de conséquence** de l'annulation que vous avez prononcée en octobre dernier, que vous avez circonscrite à la pseudonymisation des données conservées en vue d'un usage statistique.

Le décret attaqué n'avait pas à remédier à de **prétendues illégalités figurant dans le décret initial**. D'une part, un tel remède, à le supposer nécessaire, peut être apporté par n'importe quel décret, de sorte qu'il ne peut être utilement reproché à l'Etat de ne pas l'avoir fait par le décret attaqué. Le bon angle attaque est celui du refus d'abroger ou de modifier le décret initial. D'autre part, les illégalités alléguées n'existent pas. Contrairement à ce qui est soutenu, la liste des personnes autorisées à consulter les données figurant dans HOPSYWEB est précisément définie, comme le sont les destinataires de l'information sur la mise en concordance avec le FSPRT. Et il n'y avait pas lieu de prévoir des dispositions particulières pour assurer le droit à la rectification et à l'effacement des données se rapportant à des mesures de soins sans consentement invalidées par le juge judiciaire. Précisons que le Tribunal des conflits, dont nous vous avions signalé la saisine en septembre dernier, a jugé depuis qu'il n'y avait pas de place pour une annulation pour excès de pouvoir par le juge administratif de ces mesures, dont la régularité et le bien-fondé ne peuvent être appréciées que par le juge judiciaire. Il a toutefois ajouté qu'il appartenait, le cas échéant, au juge judiciaire d'en prononcer l'annulation, ce que ce dernier s'était jusqu'à présent refusé à faire, au profit de simples mesures de mainlevée pour l'avenir[32] (TC, 9 décembre 2019, *H.. –D...*, n° 4174, au Rec.). En cas d'annulation de la mesure, les données relatives au patient doivent donc être effacées, ce qui rend tout simplement sans objet la mise en relation avec le FSPRT pour ce qui le concerne.

---

mentionner dans l'acte de création du traitement. En l'occurrence, le silence du décret doit être interprété comme reconnaissant un tel droit d'information. Les patients figurant dans HOPSYWEB doivent être informés de la mise en relation et de l'information du préfet s'ils devaient aussi figurer dans le FSPRT – ce qui n'implique pas de les informer sur leur présence ou non dans le FSPRT. C'est ce qu'a demandé la CNIL dans son avis et que plaide le ministre en défense.

[31] Il est vrai que, par le passé, vous avez déjà répondu au fond à un tel moyen, sans réserver la question de son opérance (CE, 26 juillet 2006, *GISTI et autres*, n° 285714, au Rec. ; CE, 30 décembre 2009, *Association SOS Racisme, GISTI et autres*, n° 312051-313760, au Rec.) mais à bien y regarder, il s'agissait en réalité de s'intéresser à l'existence d'une habilitation des personnes autorisées à accéder aux données, ce qui se rapporte non pas aux exigences de sécurité, mais à la pertinence et, plus précisément, à la minimisation de la liste des accédants et des destinataires.

[32] Nous renvoyons sur ce point aux conclusions que nous avons prononcées le 16 septembre 2019 dans l'affaire 421329 et s.

Enfin, le moyen tiré de la méconnaissance de l'article 8 de la Charte des droits fondamentaux de l'Union européenne n'est pas assorti des précisions permettant d'en apprécier le bien-fondé.

**PCMNC à l'admission de l'intervention de l'union nationale des familles et amis de personnes malades et/ou handicapées psychiques et au rejet des requêtes.**