

## CONSEIL D'ETAT

AMPLIATION RECTIFICATIVE  
du 11 décembre 2017

Assemblée générale

Séance du jeudi 7 décembre 2017

Section de l'intérieur

N° 393836

EXTRAIT DU REGISTRE  
DES DELIBERATIONS

## 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

NOR : JUSC1732261L

*Présentation générale*

1. Saisi le 17 novembre 2017 d'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, le Conseil d'Etat observe en premier lieu que la richesse et l'ampleur du règlement (UE) 2016/679 et de la directive (UE) 2016/680 du Parlement européen et du Conseil en date du 27 avril 2016 ne permettent pas de décrire leur contenu dans le présent avis sans risquer d'en méconnaître des aspects importants. Le Conseil d'Etat souhaite cependant attirer l'attention sur deux aspects majeurs des changements qu'apportent ce règlement et cette directive dans le mode d'intervention des pouvoirs publics pour protéger les libertés fondamentales lors du traitement des données personnelles, changements dont la bonne appréhension est essentielle à la compréhension des appréciations qu'il porte sur l'équilibre du projet de loi examiné.

Auparavant, une directive de 1995 visait à harmoniser des pratiques nationales écloses dans chaque Etat, la France en premier, au fur et à mesure des évolutions. Celles-ci ont conduit à la création dans chaque Etat membre d'une ou plusieurs autorités de contrôle, aux pouvoirs inégaux d'un pays à l'autre, coordonnées par un groupe les réunissant, dénué de pouvoirs propres. Le régime de supervision des traitements reposait sur des prohibitions absolues, tempérées par un système de formalités préalables allant de la déclaration du traitement, jusqu'à son autorisation sous de strictes contraintes de procédure et de fond, proportionnées au degré d'atteinte portée par le traitement aux libertés.

Le nouveau régime opère un renversement complet des logiques antérieures.

Le champ des données à traiter ne comporte plus que de rares prohibitions absolues et invite à raisonner en termes de risques d'atteinte aux libertés et droits fondamentaux. La charge de cette

analyse n'est plus définie a priori par le législateur, imposant des contrôles progressivement durcis, mais incombe aux responsables du traitement. Ces derniers devront mener une analyse critique réalisée par un délégué à la protection des données, interne à l'organisation mais indépendant qui, chargé de faire respecter le règlement, la directive et les textes pris pour leur application, est désormais le pivot de leur respect. Dans le cas où un traitement a des effets potentiels graves, l'autorité de contrôle est saisie. Son rôle est désormais d'abord de déterminer de bonnes pratiques, en liaison avec les responsables, et de définir des référentiels, pour encadrer la création des traitements les plus communs et les harmoniser. Pour assurer le bon fonctionnement du système, l'autorité de contrôle est dotée de pouvoirs d'investigation et de sanctions renforcés.

2. Au plan européen, le système créé n'a pas de précédent ; il est différent de celui d'un modèle intégré où les autorités nationales exercent en commun une compétence de l'Union que le principe de subsidiarité délègue à leur niveau sans que l'Union se dépouille d'une compétence propre (comme dans le domaine de la concurrence). Il est également différent d'un système de coopération souple entre autorités, dans lequel les compétences nationales ne peuvent être articulées en dernière analyse que grâce au juge européen (comme dans la régulation des réseaux). Pour la protection des données personnelles, les autorités nationales voient en effet désormais leur compétence matérielle et territoriale clarifiée et l'exercice de leurs pouvoirs articulé. Une autorité peut intervenir dans deux circonstances : soit le responsable du traitement est établi sur son territoire national (tout traitement opéré à destination du territoire européen, quelles que soient ses conditions matérielles de fonctionnement, doit conduire son auteur à désigner un responsable, au sens du droit de l'Union, du traitement), soit la personne que le traitement concerne est sur son territoire. En outre, le règlement permet de trancher les conflits de compétence. Une seule autorité peut être qualifiée de chef de file pour l'exercice du contrôle sur un traitement : en principe celle sur le territoire de laquelle le responsable est établi ; les autres, dites autorités concernées, peuvent toujours intervenir, mais en respectant les prérogatives de la première. En cas de désaccord entre autorités, un comité les réunissant tranche les différends, selon des règles de majorité qualifiée qui s'assouplissent avec le temps en cas d'impossibilité de les réunir.

3. Ces évolutions significatives invitent à la plus grande vigilance d'abord dans la charge qui est désormais transférée sur les responsables de traitement : le coût économique de celle-ci, comme la responsabilité accrue qui leur est donnée, avec les risques qu'elle comporte, demandent que la loi soit la plus précise et la plus claire pour assurer un environnement robuste à leur prise de décision. Il faut assurer en même temps le maintien d'un standard élevé de protection, non seulement par l'usage, le cas échéant, des facultés reconnues aux Etats par leur droit interne de renforcer les contrôles (par exemple par des autorisations a priori), mais aussi par l'adoption des règles qui, pour relever du droit souple, doivent être claires et rigoureuses : les évolutions permises par le contrôle juridictionnel en la matière contribueront à l'atteinte de cet objectif.

La cohérence de la mise en œuvre du droit de l'Union sur l'ensemble de son territoire est également essentielle à son plein effet. Elle ne sera atteinte que par une claire répartition des compétences entre autorités, selon les critères fixés par le règlement et rappelés ci-dessus. Elle dépend aussi de la fidélité des droits nationaux aux règles posées par le règlement et la directive qui, en dépit des nombreuses marges de manœuvre laissées aux Etats-membres, doivent construire un standard européen homogène et ambitieux, capable d'influencer de bonnes pratiques au niveau mondial. Le Conseil d'Etat y veille particulièrement à l'occasion de son examen.

*Etude d'impact et consultations*

4. Le Conseil d'Etat observe, à nouveau, que l'étude d'impact n'éclaire, en dépit de son volume, qu'assez peu les choix stratégiques que le Gouvernement a pratiqués. Si chaque article fait l'objet d'une analyse détaillée, le parti de mise en œuvre du règlement, le choix d'user de certaines marges de manœuvre qu'il permet, l'insertion du texte au sein des politiques publiques dont la dimension numérique est essentielle, sont autant d'aspects que l'étude aurait dû développer. Le Conseil d'Etat remarque par ailleurs que le coût économique de la mise en œuvre du texte en particulier pour les entreprises, ainsi que ses conséquences budgétaires, pour l'Etat, ses établissements et les collectivités territoriales, n'ont pas été analysés. Il invite le Gouvernement à la plus grande attention en la matière, y compris dans les choix réglementaires qui lui incomberont.

5. C'est justement pour être complètement éclairé sur les enjeux et les conséquences du texte examiné que la section de l'intérieur du Conseil d'Etat a choisi, au cours de deux séances successives, de mener des auditions auprès d'un grand nombre d'acteurs concernés : CNIL, Conseil national du numérique, commission consultative des droits de l'homme, administrateur général des données de l'Etat, entreprises et leurs organisations représentatives. Ces auditions, qui ont été très utiles, ont mis en lumière la nécessité non seulement d'adopter rapidement le projet de loi pour respecter la date butoir du 25 mai 2018, mais aussi de concentrer tous les efforts pour informer et préparer l'ensemble des acteurs, notamment les PME, qui semblent ne pas être tous prêts aux changements profonds qu'introduit le nouveau régime issu du droit européen.

*Choix légistiques et propositions pour une meilleure lisibilité du droit*

6. Les choix légistiques faits par le Conseil d'Etat tiennent compte à la fois de la nécessité de mettre en œuvre de manière complète le droit de l'Union issu des deux instruments que sont d'une part le règlement (UE) 2016/679, applicable directement dès son entrée en vigueur le 25 mai 2018, d'autre part la directive (UE) 2016/680, qui doit être transposée avant le 6 mai 2018, et du souhait du Gouvernement de conserver comme instrument principal au niveau national la loi du 6 janvier 1978 en raison notamment de sa valeur symbolique.

7. Plutôt que de recopier le règlement, il souscrit à l'approche consistant à éliminer seulement de la loi n° 78-17 du 6 janvier 1978 celles de ces dispositions qui sont contraires au règlement et à mettre en conformité, notamment sur le plan des définitions, celles qui doivent l'être. Chaque fois que le Gouvernement souhaite utiliser l'une des 56 marges de manœuvre nationales ouvertes par le règlement, il s'efforce de réécrire les dispositions nécessaires, qu'elles soient plus exigeantes ou au contraire plus souples, plutôt que de répéter le principe posé par le règlement.

8. La directive (UE) 2016/680, qui concerne seulement les traitements de données à caractère personnel pour les autorités compétentes à des fins pénales ou de prévention et de protection contre les menaces pour la sécurité publique, doit être transposée : c'est l'objet du titre III du projet de loi. Toutefois le Conseil d'Etat constate que, bien que le règlement (UE) 2016/679, aux termes de son article 2, ne s'applique pas aux traitements de données à caractère personnel relevant du champ de la directive (UE) 2016/680, certains articles de la directive contiennent des dispositions strictement ou quasiment identiques à celles du règlement. Si la Cour de justice de l'Union européenne censure le simple renvoi général au droit de l'Union en guise de transposition (CJCE, 20 mars 1997, Commission contre Allemagne, C 96/95, Rec. p. 1653), le

Conseil d'Etat estime que des renvois précis à certaines dispositions du règlement peuvent valablement suffire à transposer des articles de la directive, notamment ceux relatifs aux définitions, à la responsabilité du sous-traitant, aux obligations de sécurité, à la coopération avec la CNIL et à la notification des violations des données personnelles. Ainsi, il est fait renvoi, au sein du nouveau chapitre XIII de la loi du 6 janvier 1978, à des articles ou subdivisions d'articles du règlement pour transposer les dispositions similaires de la directive.

**9.** Si elle est économe, la technique mise en œuvre aboutit cependant à un résultat très insatisfaisant en termes de lisibilité du droit positif. Pour y remédier, le Conseil d'Etat retient deux types de dispositions :

- en premier lieu, celle par laquelle le Gouvernement est habilité, dans un délai que le Conseil d'Etat propose de raccourcir à 6 mois, courant à compter de la publication de la loi, à procéder, par ordonnance, à une remise en forme et en cohérence non seulement de la loi de 1978, mais aussi de textes voisins et liés, sans remettre en cause les choix fondamentaux faits dans le projet de loi, de façon à garantir une meilleure accessibilité de l'ensemble du droit applicable au traitement des données personnelles, lui paraît utile et bienvenue ;

- en deuxième lieu, pour garantir, jusqu'à l'entrée en vigueur de l'ordonnance qui procédera au toilettage de la loi du 6 janvier 1978, l'accessibilité du droit, le Conseil d'Etat propose que la publication numérique à l'initiative des pouvoirs publics de la loi de 1978 soit obligatoirement opérée en étant assortie d'un lien informatique avec le texte pertinent du règlement (UE) 2016/679, chaque fois que la loi mentionne une de ses dispositions.

**10.** Le Conseil d'Etat rappelle enfin qu'il a consacré en 2014 et 2017 deux études aux questions relatives à l'impact du numérique, notamment sur les libertés. L'évolution des techniques informatiques et de leur emploi demande, pour des raisons éthiques et de protection des libertés, ensuite économiques et de compétitivité, que les pouvoirs publics adoptent sur des points essentiels des orientations aptes tant à préserver et promouvoir les valeurs et droits constitutionnels essentiels, qu'à assurer à la France et l'Europe un meilleur rang dans la compétition économique qui trouve sa source, ses moyens, et sa concrétisation dans les ressources informatiques. A ce titre, les conséquences du traitement massif des données, la propriété (ou l'inappropriabilité) et la valorisation de celles détenues ou élaborées, la maîtrise et le contrôle des algorithmes, la place de l'intelligence artificielle, les modalités d'assistance aux activités humaines procurées par les moyens informatiques, y compris en portant atteinte à l'intégrité du corps humain ou en modifiant ses capacités, devraient, indépendamment des textes européens en préparation, faire l'objet de réflexions éthiques, puis de choix politiques, susceptibles de structurer des normes juridiques robustes au regard des évolutions techniques. Le projet de loi examiné dans le présent avis n'est sans doute pas le meilleur point d'application pour cet enrichissement. Mais une telle ambition devrait animer les pouvoirs publics dans la construction d'un cadre normatif qui, d'une part, tirerait les conséquences des réflexions éthiques et des choix politiques évoqués plus haut et d'autre part, rassemblerait l'ensemble des règles applicables dans ce qui pourrait prendre la forme, si le Gouvernement souscrit à cette idée, d'un futur « code du numérique et des libertés ».

#### *Missions de la CNIL*

**11.** Le Conseil d'Etat estime nécessaire d'insérer dès le début de l'article 11 de la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, qui définit les missions de la Commission

nationale de l'informatique et des libertés (CNIL), la disposition selon laquelle celle-ci est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679.

**12.** Le Conseil d'Etat observe qu'en conformité avec ce règlement européen, la CNIL se voit attribuer le pouvoir d'adopter de nouveaux instruments de droit souple : lignes directrices, recommandations, référentiels, codes de conduite, dispositifs de certification... Il note, d'une part, que ces instruments, dont la normativité est graduée, sont adaptés au nouvel environnement juridique créé par le règlement (UE) 2016/679, qui favorise l'évaluation préalable des risques inhérents à de nombreux de traitements numériques, invite les responsables de ces traitements aux mises en conformité nécessaires et réduit les dispositifs de déclaration et d'autorisation préalables, inadaptés à la généralisation et la banalisation des usages numériques. Il se félicite, d'autre part, de ce que les enseignements et préconisations tirés de son étude annuelle de 2013 consacrée au droit souple aient été, à cette occasion, pris en considération.

#### *Commissaire du Gouvernement et formation restreinte*

**13.** Le Conseil d'Etat recommande des modifications, qui ne sont pas proposées par le projet de loi dont il est saisi, à la rédaction des articles 17 et 18 de la loi n° 78-17 du 6 janvier 1978.

Ces modifications, guidées par le souci de rehausser au niveau de la loi les garanties d'impartialité exigées par la jurisprudence constitutionnelle à propos du pouvoir de sanction des autorités administratives indépendantes (Conseil constitutionnel, décision n° 2012-280/QPC du 12 octobre 2012), ont un double objet :

- prévoir, d'une part, que le commissaire du Gouvernement, s'il peut être présent aux séances de la formation restreinte compétente pour prononcer des injonctions ou imposer des sanctions, ne peut assister au délibéré qui les suit ;
- exclure, d'autre part, de ce délibéré les agents de la commission, à la seule exception de ceux chargés du secrétariat de la séance.

#### *Contrôles*

**14.** La première modification apportée par le projet de loi concerne la nature des locaux dans lesquels les agents de la CNIL peuvent procéder à des contrôles sur place. Elle étend la possibilité de tels contrôles, de 6 heures à 21 heures, à l'ensemble des locaux qui ne sont pas affectés, en tout ou en partie, au domicile privé. La notion « d'usage professionnel » à laquelle recourt la rédaction actuelle du I de l'article 44 de la loi du 6 janvier 1978 se prête aujourd'hui à des difficultés d'interprétation, lorsque les matériels sont installés, par exemple, dans un couloir, dans un espace mixte ou partagé avec d'autres utilisateurs. Le Conseil d'Etat n'émet pas d'objection à cette nouvelle rédaction, dans la mesure où le II de l'article 44 offre, au regard des finalités légitimes poursuivies par le contrôle et la nature des locaux visités, qui exclut le domicile, des garanties appropriées (information du responsable de son droit d'opposition, autorisation du juge des libertés et de la détention en cas d'opposition, assistance d'un conseil, recours contre l'autorisation et de déroulement des opérations de visite).

**15.** La deuxième modification concerne le secret professionnel opposable aux membres ou agents de la CNIL dans l'exercice des contrôles, qui fait l'objet d'une définition plus précise à laquelle souscrit le Conseil d'Etat.

**16.** A ce titre, si la nouvelle rédaction n'exige plus, pour les données couvertes par le secret médical, que leur communication soit nécessairement requise par un médecin, elle dispose, grâce à une précision apportée par le Conseil d'Etat, que cette communication ne peut être faite que sous l'autorité et en présence du médecin. Le terme « d'autorité » proposé par le Conseil d'Etat signifie que l'agent menant le contrôle sera placé sous la responsabilité fonctionnelle du médecin, qui ne réalisera pas nécessairement lui-même les opérations informatiques mais adressera toutes les instructions nécessaires à l'agent pour que ne soit pas violé le secret médical.

**17.** Le projet de loi prévoit que les agents de la CNIL chargés du contrôle pourront utiliser une identité d'emprunt : ils pourront, par exemple, utiliser pour les contrôles en ligne une adresse électronique qui n'est pas celle de la CNIL, associée ou non à un autre nom ou à un pseudonyme. Cette mesure, dont bénéficient déjà les agents de l'Autorité des marchés financiers, est de nature à renforcer l'efficacité des contrôles en ligne et doit faire l'objet d'une autorisation expresse du législateur, afin de prémunir ces contrôles du risque de contestations fondées sur violation du principe de loyauté dans la collecte des preuves.

**18.** Enfin, en conformité avec le règlement et la directive, il est nécessaire de préciser que la CNIL n'est pas compétente pour contrôler les opérations de traitements effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions.

#### *Modalités de coopération entre autorités de contrôle européennes*

**19.** Le règlement (UE) 2016/679 prévoit, à son article 62, que lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs Etats-membres ou si un nombre important de personnes concernées dans plusieurs Etats-membres sont susceptibles d'être sensiblement affectées par des opérations de traitement, une autorité de contrôle de chacun de ces Etats-membres a le droit de participer aux opérations conjointes menées sur le territoire des différents Etats. L'autorité de contrôle compétente doit alors inviter l'autorité de contrôle de chacun de ces Etats-membres à prendre part aux opérations conjointes concernées.

Si le règlement de l'Union laisse au droit national une certaine marge de manœuvre pour définir les pouvoirs d'enquête qui peuvent être confiés aux membres et agents ainsi associés aux opérations conjointes, le Conseil d'Etat estime préférable, à la différence du projet dont il est saisi qui limite le rôle de ces membres ou agents à une simple présence passive, de donner au président de la CNIL une certaine latitude : la rédaction adoptée par le Conseil d'Etat permet au président d'habiliter, par décision particulière, ceux des membres ou agents de l'autorité de contrôle concernée qui présentent des garanties comparables à celles requises des agents de la CNIL. Les contrôles auxquels participeront ces agents habilités, qui ne disposeront pas de pouvoirs plus étendus que ceux confiés à leurs homologues français, seront exercés sous l'autorité de la CNIL. Entourée ainsi des garanties nécessaires, la disposition paraît au Conseil d'Etat de nature à renforcer l'efficacité des contrôles et à inciter les autres autorités de contrôle européennes à adopter le même standard, sans se heurter à un obstacle constitutionnel, s'agissant au surplus d'enquêtes de nature administrative.

**20.** Lorsque la coopération entre les autorités de contrôle conduit à ajouter un grief ou à revoir une qualification qui ne figurait pas dans l'acte de notification des griefs, la procédure contradictoire doit pouvoir se poursuivre, conformément au principe constitutionnel issu de l'article 16 de la Déclaration des droits de l'homme et du citoyen et aux stipulations de l'article 6 de la convention européenne des droits de l'homme. Les particularités de la coopération entre autorités de contrôle conduisent à compléter le projet de loi sur ce point et prévoir que seront

définies par un décret en Conseil d'Etat les conditions dans lesquelles le caractère contradictoire de la procédure est garanti à l'égard du ou des responsables de traitement et sous-traitants et les modalités de communication des pièces du dossier durant la procédure.

### *Formalités préalables*

**21.** Concernant les dispositions du chapitre II du projet de loi relatives à la simplification des formalités préalables à la mise en œuvre des traitements, le Conseil d'Etat écarte la disposition introduite par le Gouvernement à des fins pédagogiques et de lisibilité, qui se borne à recopier les dispositions du règlement (UE) 2016/679 (article 36), qui sont d'application directe, prévoyant que le responsable du traitement consulte la CNIL préalablement à ce traitement, lorsqu'une analyse d'impact révèle que celui-ci présenterait un risque élevé si le responsable ne prend pas les mesures requises pour atténuer ce risque.

**22.** Au regard de l'enjeu de la protection des données, le projet de loi conserve un régime d'autorisation préalable pour les traitements mis en œuvre qui portent sur trois types de données : pour le compte de l'Etat, les données biométriques et les données génétiques et, pour le compte de personnes publiques ou privées, les données comportant le numéro d'inscription des personnes au Répertoire national d'identification des personnes physiques (NIR). S'agissant plus particulièrement des traitements qui comportent le NIR, un décret en Conseil d'Etat doit déterminer les catégories de responsables de traitement et les finalités autorisées de ces traitements. L'autorisation n'est pas requise pour les traitements qui ont exclusivement des finalités de statistique publique, de recherche scientifique ou historique ou qui mettent à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique. Le numéro d'inscription au répertoire national d'identification des personnes physiques fait préalablement l'objet d'une opération cryptographique lui substituant un code statistique non significatif.

**23.** Pour ce qui est des données de santé utilisant le NIR, elles sont soumises aux formalités prévues au chapitre IX de la loi n° 78-17 du 6 janvier 1978 « Traitement de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé », à l'exception des traitements portant sur les alertes sanitaires qui seront, quant à elles, soumises au droit commun de l'analyse d'impact ou, lorsqu'elles utilisent le NIR, au régime d'autorisation prévu par le décret-cadre précité.

**24.** Enfin, compte tenu de la logique générale du règlement fondée sur une responsabilisation des acteurs et un maintien de garanties en cas de risque élevé pour la protection des données personnelles, le projet de loi supprime logiquement le régime déclaratif prévu aux articles 22 à 24 de la loi n° 78-17 et abroge les articles 24 et 25 de la même loi.

### *Délégué à la protection des données*

**25.** Le projet dont est saisi le Conseil d'Etat se propose d'abroger les dispositions des III et IV de l'article 22 de la loi du 6 janvier 1978. Les premières régissent le rôle du correspondant à la protection des données, dont l'institution dispense aujourd'hui les responsables de traitement des formalités des articles 23 et 24 de cette loi. Les secondes traitent une catégorie de données non concernées par la loi 1978, qui n'a plus de raison d'être, en raison de l'ampleur du champ du règlement. Le Conseil d'Etat écarte les dispositions par lesquelles le Gouvernement entendait incorporer dans la loi la création de la fonction de délégué à la protection des données, ainsi que

l'obligation de tenir un registre pour le traitement. En effet, ces obligations sont très précisément définies par les articles 37 et suivants du règlement (UE) 2016/679, qui assurent aussi par leur application directe la transposition des obligations que la directive impose aux Etats aux articles 32 et suivants. D'application directe, ces dispositions n'appellent aucune précision autre que l'abrogation des dispositions contraires existantes. Au surplus, les précisions que donnait le Gouvernement n'étaient que partielles, et auraient laissé planer une incertitude sur le motif pour lesquels d'autres caractéristiques des délégués ou de leurs fonctions ne faisaient pas l'objet d'une reprise par la loi nationale.

**26.** Le projet dont est saisi le Conseil d'Etat envisage d'ajouter à l'article 35 de la loi du 6 janvier 1978, qui décrit le régime et les obligations du sous-traitant d'un traitement, l'obligation pour ce sous-traitant de se conformer au chapitre 4 du règlement de l'Union. Or, les dispositions de l'article 35 sont en retrait par rapport à l'ensemble des obligations que non seulement le chapitre 4, mais l'ensemble du règlement impose aux sous-traitants d'un traitement. Le Conseil d'Etat estime donc préférable d'abroger ces dispositions, ce qui aura pour effet de rendre directement applicables sans aucun obstacle l'ensemble des dispositions du règlement relatives aux sous-traitants, et ainsi d'assurer complètement la transposition de la directive.

#### *Données d'infraction*

**27.** Le projet de loi procède à l'ajustement de la rédaction de l'article 9 de la loi du 6 janvier 1978 afin d'harmoniser sa terminologie. Il remédie également aux conséquences de la décision n° 2004-499 DC du Conseil constitutionnel du 29 juillet 2004 qui a censuré l'incompétence négative entachant les dispositions du 3° de cet article 9, faute pour le législateur d'avoir précisé dans quelles conditions et limites les personnes souhaitant, pour assurer la défense de leurs droits devant un juge, traiter ce type de données à caractère pénal concernées par cet article, pouvaient y procéder. Les précisions apportées, s'inspirant directement des réserves d'interprétation ayant entraîné la censure par le juge constitutionnel, n'appellent pas de réserve. Enfin ce nouvel article comporte des dispositions encadrant la réutilisation des données issues de jugements. Bien que ceux-ci soient, en principe, anonymisés lorsqu'ils sont communiqués au public, et que les articles 20 et 21 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique imposent une étude préalable aux fins de vérifier la possibilité de réidentification des personnes lors de la communication, le Conseil d'Etat estime qu'il est opportun de donner une base légale à ce type de traitement, afin d'éviter qu'une levée d'anonymat partielle, fortuite ou involontaire, résultant notamment d'un traitement massifié de données, aboutissant à traiter des données personnelles à caractère pénal, ne puisse faire obstacle au recours aux techniques numériques au service du droit par les différents utilisateurs.

**28.** Le projet de loi se propose d'adapter la rédaction des dispositions de l'article 36 de la loi du 6 janvier 1978 relatives à la conservation des données au-delà des nécessités du traitement les concernant à des fins historiques, statistiques, ou scientifiques. Mais les dispositions prévues se bornaient à harmoniser partiellement le vocabulaire et les règles, pour les aligner sur le règlement auquel il était renvoyé, et à prévoir que d'autres dispositions, législatives et réglementaires, mettraient en œuvre les possibilités de dérogation et les garanties prévues notamment à l'article 89 du règlement (UE) 2016/679. La combinaison des articles 5 et 89 du règlement définissant parfaitement les conditions dans lesquelles des données à caractère personnel peuvent être conservées au-delà des durées légales initialement prévues, à des fins d'utilisation archivistique, scientifique ou statistique, le Conseil d'Etat préfère recommander l'abrogation pure et simple de l'article 36 de la loi de 1978 au profit du régime directement issu du règlement.



Il existe cependant, dans le domaine couvert par la dérogation permise par le règlement, une autonomie des traitements à des fins archivistiques : il est ici possible d'utiliser les facultés reconnues par le règlement, car le champ des traitements concernés est strictement fixé par la loi (article L. 211-2 du code du patrimoine) aussi bien quant à son objet que quant à ses finalités, tandis que le régime tant législatif que réglementaire applicable offre de nombreuses garanties quant aux modalités de mise en œuvre de ce traitement (qualification des personnels, méthode...). Dès lors, il est possible d'énoncer que l'ensemble des traitements concernés (qui, d'ailleurs, ne font pas l'objet d'actes individuels de création, mais constituent globalement la mise en œuvre de la mission archivistique) font l'objet de la dérogation permise aux articles 15,16 et 18 à 21 du règlement de l'Union, concernant pour l'essentiel les droits d'information et d'opposition des personnes concernées, dans la limite de la contrariété de ces droits aux finalités du traitement. Le Conseil d'Etat retient donc la rédaction qui est adéquate à ce domaine dans le nouvel article 36 de la loi de 1978.

### *Données de santé*

**29.** Le Gouvernement a choisi d'employer les facultés qui lui sont reconnues par le règlement pour le traitement des données de santé (notamment à l'article 23 du règlement (UE) 2016/679).

Le régime propre à ces traitements, décrit par les nouveaux articles 53 à 63 de la loi du 6 janvier 1978, en exonère certains d'entre eux, qu'ils soient par exemple destinés à l'administration de la sécurité sociale ou créés dans des conditions préservant les droits et libertés fondamentales par nature, ou qu'ils répondent aux nécessités d'une situation d'urgence en cas de crise sanitaire. Ce régime prévoit la création de référentiels par la CNIL. L'attestation de s'y soumettre suffit à permettre la mise en œuvre de ce traitement. A défaut, l'autorisation de la CNIL est nécessaire, le cas échéant articulée avec l'Institut national des données de santé et, en matière de recherche, avec les comités créés par le code de la santé publique à cette fin. La décision de la CNIL doit intervenir dans le délai de deux mois à l'expiration desquels, sauf prolongation prévue par la loi, la décision est réputée favorable. Le Conseil d'Etat observe que les conséquences de ce régime de décision implicite sur les moyens humains et matériels de la CNIL n'ont pas fait l'objet d'une analyse de la part du Gouvernement qui devra veiller à ce que cette commission dispose des moyens de prendre effectivement position au regard de l'importance et du nombre de ces traitements.

Le régime applicable aux données de santé est ainsi conforme au règlement de l'Union et reprend largement celui existant aujourd'hui dans le chapitre 9 de la loi. Sans formuler de réserves sur ce choix, le Conseil d'Etat appelle le Gouvernement à apporter un soin particulier à l'articulation de ce régime avec celui issu de la loi du 26 janvier 2016 ayant modifié le code de la santé publique, dont les décrets d'application viennent d'être pris.

**30.** Le règlement de l'Union, en dehors du champ des services, laisse aux Etats le soin de déterminer l'âge légal du consentement au traitement de données. Dans ce domaine, l'information des personnes exerçant, sur les mineurs, l'autorité parentale, à l'occasion et par voie de conséquence du recueil de leur consentement au traitement des données personnelles de santé d'un mineur, peut aboutir à révéler des informations personnelles. Le législateur a déjà admis que ces révélations pouvaient être préjudiciables aux intérêts du mineur et a, pour ce motif, autorisé que, par exemple, des professionnels de santé n'en fassent pas état (articles L. 1111-5 et suivant du code de la santé publique). Il est en effet particulièrement dommageable pour les intérêts des mineurs qu'à raison de la simple inclusion, dans un traitement informatique, des

éléments relatifs à la santé susceptibles d'entraîner des conséquences très négatives dans la relation avec le mineur puissent être portés à la connaissance des parents (informations relatives à des traitements en lien avec les addictions, ou les relations et l'orientation sexuelle, notamment). Au regard de cet objectif, le Gouvernement a choisi de confirmer le choix fait récemment par le législateur, lors de l'adoption de l'article 56 de la loi du 7 octobre 2016 pour une République numérique, de fixer à 15 ans l'âge du consentement des mineurs à un traitement de leurs données personnelles de santé. Pour ce motif, le Conseil d'Etat se borne à remarquer qu'il incombera au Gouvernement de veiller à mettre en cohérence ces dispositions avec celles des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique. Alors, en effet, que le recueil du consentement des parents au traitement des données de santé de leurs enfants de moins de 15 ans entraînera nécessairement leur information sur les données de santé objet du traitement, ces articles permettent aux médecins, sages-femmes et infirmiers, s'ils ne sont pas parvenus à persuader un mineur de les laisser recueillir l'accord de leur parent à des actes de santé, d'y procéder avec le seul consentement des mineurs, ce qui leur interdit d'en informer les parents. Délicate à opérer, car le processus de dialogue d'un professionnel de santé avec un patient n'est pas de même nature que celui de recueil de consentement à un traitement de données par son responsable, cette articulation n'en est pas moins nécessaire.

#### *Consentement des mineurs pour les autres traitements de données*

**31.** Le règlement (UE) 2016/679 introduit, par la combinaison de ces articles 6, 7 et 8, le principe de dispositions spécifiques destinées à protéger les enfants, reposant notamment sur leur consentement exprès au traitement de données personnelles les concernant dans certains cas. Le règlement fixe l'âge de ce consentement à 16 ans pour l'accès à des services, mais permet aux Etats d'abaisser cette limite jusqu'à 13 ans.

**32.** Le Gouvernement entend introduire un article 7 *bis* dans la loi de 1978 manifestant son choix de ne pas modifier le principe de consentement à 16 ans (sans préjudice du cas, relevant d'un autre ordre de dispositions, des données médicales traitées ci-dessus). Tout en reconnaissant l'inutilité de cette disposition, il estime qu'elles contribuent à la sécurité juridique, notamment pour la détermination des règles territorialement applicables. Il entend aussi pouvoir soumettre expressément ce choix au Parlement.

**33.** Comme déjà indiqué plus haut aux paragraphes 6 et suivants du présent avis, la recopie seulement partielle de dispositions du règlement créerait plus d'insécurité juridique qu'elle ne la réduirait. Conformément aux choix légistiques expliqués dans le présent avis (§ 6 et suivants), le Conseil d'Etat écarte donc cette disposition.

#### *Algorithmes*

**34.** L'article 10 de la loi du 6 janvier 1978 limite la possibilité de prise de décision sur le seul fondement d'un traitement informatique appréciant la personnalité du destinataire, sous réserve de quelques exceptions. Le règlement (UE) 2016/679 rend désormais possible le recours aux traitements, prenant acte de l'importance des algorithmes et des techniques de profilage. Il ne rend cependant ce recours possible que soit avec le consentement des intéressés, soit pour la conclusion ou l'exécution d'un contrat, soit sur la base d'une disposition européenne ou nationale en ce sens, à condition qu'alors la préservation des droits et libertés soit assurée. La loi pour une République numérique du 7 octobre 2016 avait anticipé sur cette dernière autorisation en posant le principe qu'une décision administrative pouvait être prise sur le fondement d'un

algorithme, puisqu'elle prévoyait dans ce cas l'ouverture d'un droit à information sur le contenu et le fonctionnement de l'algorithme.

**35.** Le Gouvernement se propose de reprendre ce principe de limitation, en réservant cette possibilité de prise de décision, sous réserve des deux exceptions de droit, aux seules décisions administratives individuelles.

Mais la garantie apportée par le projet de loi se borne à l'information prévue par l'article L. 311-3-1 du code des relations du public avec l'administration. Même si ce code pose par ailleurs un principe de maîtrise par l'administration de systèmes informatiques, le Conseil d'Etat estime nécessaire de poser, au nombre des mesures appropriées évoquées par le règlement de l'Union, le principe selon lequel le responsable du traitement, dans le cas où celui-ci comporte un algorithme qui peut-être à l'origine d'une décision administrative individuelle, est tenu de se donner les moyens de maîtriser l'algorithme et de documenter, notamment à destination de l'autorité de contrôle, les actions entreprises à cette fin. Il est en effet essentiel, alors même qu'il n'est plus nécessaire que l'action humaine s'interpose entre le traitement et la prise de décision, de garantir à tout instant une maîtrise humaine complète des algorithmes, comportant notamment la capacité d'interrompre le fonctionnement du traitement, notamment lorsque ceux-ci sont dotés de capacités d'apprentissage leur permettant de modifier leur logique de fonctionnement sans une démarche humaine préalable de validation. Le rappel de ce principe n'est conçu que comme un premier pas vers la définition d'un régime plus complet du contrôle des algorithmes, y compris au-delà du champ des décisions administratives individuelles, qui apparaît de plus en plus nécessaire.

#### *Traitements mis en œuvre par l'Etat*

**36.** Le Gouvernement entend user, au profit des traitements mis en œuvre par l'Etat, de la faculté que lui reconnaît l'article 23 du règlement (UE) 2016/679 de déroger à la plupart des droits garantis au profit des destinataires d'un traitement pour des motifs d'intérêt général largement définis, à condition d'entourer cette dérogation des garanties nécessaires la préservation des droits et libertés fondamentales.

Mais la simple reproduction, au demeurant incomplète, du dispositif de l'article 23 du règlement de l'Union apparaît au Conseil d'Etat comme étant à la fois inutile et incertaine. Elle risque surtout d'entacher d'incompétence négative l'intervention du législateur en renvoyant trop généralement à des dispositions réglementaires pour définir les droits reconnus aux personnes concernées.

Le Conseil d'Etat écarte pour ces motifs les dispositions envisagées, mais il admet en revanche un premier cas de mise en œuvre de la faculté de l'article 23 : pour les seuls traitements répondant à une obligation légale, et aux seules fins de protection de la sécurité nationale, de la défense nationale ou de la sécurité publique, le seul droit à être informé des violations d'un traitement de données personnelles, régi par l'article 34 du règlement, peut être restreint par l'acte créant ce traitement. L'effet concret de ces dispositions est de permettre aux responsables du traitement de ne pas prévenir la personne dont les données ont fait l'objet d'une violation par un tiers dans des conditions mettant en cause, à raison de données ou à raison de l'emploi de la personne (par exemple s'il s'agit d'un agent des forces de sécurité ou d'un militaire), la sécurité ou la défense, afin de mieux assurer la lutte contre les auteurs de ces violations. L'intervention du législateur pour aménager une garantie à l'exercice des libertés publiques est justifiée. Elle est

suffisamment précise pour permettre un contrôle de l'adéquation de la restriction aux finalités poursuivies.

#### *Transfert de données personnelles vers un pays tiers*

**37.** Le projet comporte l'adjonction d'un article 43 *quinquies* à la loi du 6 janvier 1978, afin d'assurer la mise en conformité du droit national avec le point 65 de l'arrêt C-362/14 du 6 octobre 2015 de la Cour de justice de l'Union européenne.

**38.** Tant dans le régime résultant de la directive de 1995, que dans celui issu du règlement (UE) 2016/679, la Commission accepte que des données personnelles puissent être transférées vers un Etat tiers à l'Union, si le degré de protection de ces données dans cet Etat tiers est adéquat au standard européen, en prenant une décision dite d'adéquation. Cependant, toute personne a le droit de contester le transfert de ces données en estimant qu'elle viole ses droits, et doit pouvoir en saisir l'autorité de contrôle. Le processus conduisant alors à suspendre le transfert de ces données méconnaît nécessairement la décision d'adéquation. C'est pourquoi l'arrêt du 6 octobre 2015 de la Cour de justice exige que le droit national permette de saisir une juridiction qui, seule, est dans ce cas en mesure de poser à la Cour de justice de l'Union européenne la question préjudicielle relative à la validité de la décision d'adéquation.

**39.** Pour assurer la mise en œuvre de cette exigence, le projet du Gouvernement prévoit que saisie d'une telle contestation, la CNIL doit, si elle entend y donner suite, saisir le Conseil d'Etat d'une demande de suspension provisoire du transfert des données. Comme la commission supérieure du Conseil d'Etat l'a relevé, la rédaction retenue par le Gouvernement peut laisser entendre que la question préjudicielle n'est pas alors obligatoire : par conséquent, le Conseil d'Etat précise qu'elle doit être posée, à peine d'irrecevabilité de la demande de suspension provisoire du transfert. Et il prévoit que la CNIL peut agir de son propre chef, sans attendre une réclamation. Il étend enfin le champ de ce mécanisme aux traitements relevant de la directive (UE) 2016/680 autres que ceux relatifs à l'activité juridictionnelle.

#### *En ce qui concerne le titre III relatif à la transposition de la directive (UE) 2016/680*

**40.** Le Conseil d'Etat estime que le projet de loi opère, dans un nouveau chapitre XIII de la loi du 6 janvier 1978 qui devra être précisé par des dispositions réglementaires, une transposition complète de la directive (UE) 2016/680, à laquelle il n'apporte de compléments que sur quelques points spécifiques.

#### *Données sensibles*

**41.** Le Conseil d'Etat estime notamment nécessaire de transposer expressément l'article 10 de la directive sur les règles encadrant le traitement des données sensibles, car l'interdiction du traitement de telles données prévue à l'article 8 de la loi du 6 janvier 1978 n'est pas applicable en vertu du dernier alinéa de cet article aux traitements de l'article 26 de cette loi auquel le nouvel article 70-3 renvoie pour ceux relevant du champ de la directive.

#### *Décision individuelle automatisée*

42. Le Gouvernement ne souhaitant pas que le droit national permette, dans le champ de la directive de prendre des décisions fondées exclusivement sur un traitement automatisé de données, le Conseil d'Etat estime que l'article 11 de la directive est correctement transposé par la reprise des interdictions qui figurent à l'article 10 de la loi du 6 janvier 1978, sans les dérogations qui y sont apportées par le présent projet de loi. Il considère que le paragraphe 3 de cet article 11 relatif à l'interdiction de tout profilage entraînant une discrimination sur la base des catégories des données sensibles doit aussi être transposé expressément et il amende en ce sens le projet de loi.

*Formalités préalables à la création des traitements de données relevant du champ de la directive*

43. Le Conseil d'Etat constate que les traitements de données à caractère personnel entrant dans le champ de la directive (UE) 2016/680 sont, jusqu'à présent, soit créés après autorisation de la CNIL, soit, pour ceux mis en œuvre pour le compte de l'Etat, créés par un arrêté ministériel ou un décret en Conseil d'Etat après avis de la CNIL. Le troisième paragraphe de l'article 1<sup>er</sup> de la directive prévoyant que les Etats-membres peuvent apporter des garanties plus étendues pour la protection des droits et libertés des personnes concernées et son considérant 15 indiquant que l'application de la directive ne devrait pas conduire à un affaiblissement des garanties déjà offertes par la législation des Etats-membres, le Conseil d'Etat estime qu'il est possible, sans procéder à une « sur-transposition », de maintenir la création des traitements de données entrant dans le champ de la directive et mis en œuvre pour le compte de l'Etat, par un arrêté ministériel ou un décret en Conseil d'Etat après avis de la CNIL, conformément à l'article 26 de la loi du 6 janvier 1978. Si, conformément à la directive, il est possible de ne prévoir désormais aucune formalité préalable à la création des traitements qui ne sont pas mis en œuvre pour le compte de l'Etat, le Conseil d'Etat considère toutefois qu'il résulte de l'article 27 de la directive, qui impose une analyse d'impact préalable lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, que peut être prévue au nouvel article 70-4 de la loi du 6 janvier 1978, en cas de traitement de données sensibles au sens de l'article 8 de cette loi, la réalisation systématique d'une telle analyse d'impact. Le Conseil d'Etat estime, en outre, que, pour les traitements qui ne sont pas mis en œuvre pour le compte de l'Etat, cette dernière hypothèse devrait logiquement conduire à une consultation préalable de la CNIL sur le fondement du 1<sup>o</sup> du paragraphe 1 de l'article 28 de la directive. Dès lors, il semble au Conseil d'Etat qu'une telle transposition de la directive ne conduira pas à une diminution des garanties existant actuellement pour les traitements de données entrant dans son champ.

*Traitements de données relevant à la fois du champ de la directive et de celui du règlement ou du droit interne*

44. Le Conseil d'Etat constate qu'il existe des traitements de données à caractère personnel qui relèvent à la fois du champ de la directive, en raison de certaines de leurs finalités, et du champ du règlement (UE) 2016/679 ou du droit interne, en raison de leurs autres finalités. Cette situation est traitée par l'article 9 de la directive (UE) 2016/680, qui dispose que le traitement à d'autres fins de données collectées dans le champ de la directive n'est possible que si un tel traitement est autorisé par le droit de l'Union ou le droit de l'Etat-membre et que, dès lors que les données sont traitées à d'autres fins, le règlement s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.

45. D'une part, le Conseil d'Etat en conclut que, lorsqu'un traitement de données répond à des finalités mixtes, il convient que sa mise en œuvre soit prévue par un acte législatif ou réglementaire ou un acte répondant aux exigences de clarté, de précision et de prévisibilité rappelées au considérant 33 de la directive. Le Conseil d'Etat relève d'ailleurs que l'existence d'un tel acte est également nécessaire, lorsqu'il est envisagé d'apporter des restrictions aux droits des personnes concernées en application des articles 13, 15 et 16 de la directive, transposés à l'article 70-21 de la loi du 6 janvier 1978.

46. D'autre part, le Conseil d'Etat estime que l'article 9 de la directive impose un double régime aux traitements de données à finalités mixtes.

47. S'agissant des traitements relevant à la fois du champ de la directive et de celui du règlement, ce double régime paraît complexe à mettre en œuvre pour les droits des personnes concernées. Le Conseil d'Etat relève en effet qu'existent deux droits prévus par le règlement et absents de la directive : le droit à l'oubli (article 17 du règlement) et le droit à la portabilité des données (article 20 du règlement). Dans les deux cas, le règlement prévoit que ces droits ne sont pas applicables, lorsque le traitement est nécessaire « à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ». Ces droits devraient donc être inapplicables aux traitements de données dont les finalités sont mixtes. Les autres droits des personnes concernées (information, accès, opposition...) sont plus ouverts dans le règlement que dans la directive. Le Conseil d'Etat estime que, dès lors que les données sur lesquelles la personne concernée demande à exercer ses droits ne pourront pas être exclusivement rattachées soit aux finalités prévues par la directive, soit aux autres finalités du traitement de données, il convient que l'acte ayant autorisé le traitement de données à finalités mixtes s'appuie sur l'article 23 du règlement, qui permet une diminution de la portée des droits de la personne concernée sous plusieurs conditions, dont la sécurité publique et la préservation des procédures pénales, afin de déterminer un régime des droits des personnes concernées cohérent pour l'ensemble des données traitées pour les diverses finalités. Pour être conforme aux exigences du second paragraphe de l'article 23 du règlement, les dispositions apportant de telles limitations doivent être précises et ne sauraient prendre la forme d'habilitations générales.

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.

#### *Traitement des antécédents judiciaires*

49. Le Gouvernement saisit l'occasion du projet de loi pour y insérer des dispositions tirant les conséquences de la décision du Conseil constitutionnel n° 2017-670 QPC du 27 octobre 2017, par laquelle ce dernier a déclaré non conformes à la Constitution les dispositions de l'article 230-8 du code de procédure pénale, en tant que les modalités d'effacement des données saisies dans le fichier de traitement des antécédents judiciaires (TAJ), régies par cet article, ne permettaient de procéder à cet effacement que dans certains cas. Sur le fond, le Gouvernement remédie à la censure du Conseil constitutionnel en ouvrant désormais le droit à toute personne dont des données personnelles figurent dans le TAJ à en demander l'effacement, non seulement dans les cas déjà prévus, mais aussi dès que la condamnation pénale concernée disparaît du bulletin n° 2 du casier judiciaire. Ce choix paraît à la fois équilibré et pertinent : il est approuvé par le Conseil d'Etat.

*Application outre-mer*

**50.** La technique de transposition choisie a une conséquence inattendue sur l'application de la loi du 6 janvier 1978, telle que modifiée par la présente loi, dans les collectivités du Pacifique, ainsi que dans les Terres australes et antarctiques, à Saint-Pierre-et-Miquelon et à Saint-Barthélemy. Le droit de l'Union ne s'applique pas dans ces territoires : or la loi de 1978 n'a désormais de sens que combinée avec les dispositions d'effet direct du règlement (UE) 2016/679. Pour remédier à cette difficulté, le Conseil d'Etat ne retient pas le choix d'une disposition rendant applicable dans ces territoires une partie du règlement : l'ampleur de la modification rendrait en effet nécessaire une consultation des collectivités intéressées. Il est donc préféré, même si cette solution n'est pas entièrement satisfaisante, de s'en tenir à l'application dans ces collectivités de la loi du 6 janvier 1978 dans son état antérieur et de renvoyer à la future ordonnance à prendre dans les six mois à compter de la loi d'habilitation, le soin de procéder pour ces collectivités aux adaptations nécessaires.

*Entrée en vigueur*

**51.** Le règlement entre en vigueur le 25 mai 2018 et la directive, qui ne peut être complètement transposée tant que le règlement n'est pas en vigueur, doit pourtant l'être au plus tard le 6 mai. Le Conseil d'Etat repousse par conséquent au 25 mai 2018 l'entrée en vigueur de la loi.

*Cet avis a été délibéré par l'assemblée générale du Conseil d'Etat dans sa séance du jeudi 7 décembre 2017.*