

Commission nationale de l'informatique et des libertés

Délibération n° 2019-055 du 9 mai 2019 portant avis sur un projet de décret pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (saisine n° AV 19008103)

NOR : CNIX1915826S

La Commission nationale de l'informatique et des libertés,

Saisie par la Garde des Sceaux, ministre de la justice, d'une demande d'avis concernant un projet de décret pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la 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 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 71 ;

Vu l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Mme Marie-Laure DENIS, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Émet l'avis suivant :

1. La Commission a été saisie pour avis, le 17 avril 2019, d'un projet de décret pris pour l'application de la loi n° 78-17 du 6 janvier 1978, dans sa rédaction résultant de l'ordonnance n° 2018-1125 du 12 décembre 2018.

2. Ce projet de décret a pour objet de poursuivre la mise en conformité du droit national avec le règlement (UE) 2016/679 (ci-après « le Règlement » ou « le RGPD ») et la directive (UE) 2016/680 (ci-après « la Directive ») du 27 avril 2016. Au niveau législatif, l'adaptation du droit français au nouveau cadre européen a été finalisée par

l'adoption de l'ordonnance précitée du 12 décembre 2018, qui a réécrit la loi « Informatique et Libertés », et dont il est prévu que les dispositions entrent en vigueur en même temps que le décret d'application de la loi « Informatique et Libertés » dans sa nouvelle rédaction, et au plus tard le 1^{er} juin 2019. Le présent projet de décret vise ainsi à achever, au niveau réglementaire, ce travail d'adaptation au droit de l'Union, en abrogeant le décret n° 2005-1309 du 20 octobre 2005 susvisé et en réécrivant l'ensemble des dispositions réglementaires d'application de la loi « Informatique et Libertés ».

3. A titre liminaire, la Commission estime que ce projet de décret opère la mise en cohérence nécessaire de ces dispositions réglementaires au regard du droit européen et des dispositions législatives nationales prises en son application. En outre, il améliore substantiellement la lisibilité des différents régimes applicables en fonction de la nature des traitements concernés, notamment en distinguant les dispositions communes à tous les traitements et les exigences spécifiques au champ du Règlement, à celui de la Directive et aux traitements ne relevant pas du champ d'application du droit de l'Union. Ce projet de décret complète ainsi utilement, au niveau réglementaire, le travail de réécriture et de clarification de l'état du droit résultant de l'entrée en application des nouveaux textes européens opéré par l'ordonnance précitée du 12 décembre 2018.

4. Il appelle néanmoins les observations suivantes de la part de la Commission, étant précisé que, pour en faciliter la lecture, ces dernières ne font référence à la loi du 6 janvier 1978 modifiée que dans sa rédaction résultant de l'ordonnance précitée.

Sur les dispositions relatives au fonctionnement de la Commission

5. A titre général, les dispositions de la section 1 du chapitre Ier du Titre Ier du projet de décret clarifient utilement les modalités d'exercice des missions de la Commission et apportent les précisions et adaptations nécessaires aux règles de procédure applicables à la composition et à son fonctionnement. La Commission estime néanmoins qu'elles seraient utilement complétées des deux points suivants.

6. **En premier lieu**, la Commission estime qu'il serait opportun que le projet de décret clarifie et harmonise les conditions de publicité de certaines décisions de la formation plénière, en particulier concernant ses avis sur les projets de texte du Gouvernement. En effet, les dispositions législatives et réglementaires en vigueur prévoient déjà la publication des avis de la Commission sur les projets de loi relatifs à la protection des données à caractère personnel ou au traitement de telles données, sur les projets de texte réglementaire relatifs à des traitements devant faire l'objet de formalités préalables auprès de la Commission, ainsi que sur les projets de décret ou d'arrêté prévus par une loi imposant un avis de la Commission sur ces textes, mentionnés à la dernière phrase de l'article 8-I-4^o-a) de la loi du 6 janvier 1978 modifiée.

7. Au regard de l'impératif de transparence de l'action de la Commission, réaffirmé par plusieurs initiatives législatives récentes, il serait utile que le projet de décret prévoie également la publication des autres avis de la Commission, à l'exception de ceux ne devant pas faire l'objet d'une publication en application du III de l'article 31 de la loi « Informatique et Libertés », et en particulier des avis sur les projets de décret relatifs

à la protection des données à caractère personnel ou au traitement de telles données, au sens de la première phrase de l'article 8-I-4^o-a) de la loi du 6 janvier 1978 modifiée.

8. A cet égard, la Commission estime que la dernière phrase de ce même article 8-I-4^o-a), qui prévoit que sont publiés les avis de la CNIL sur les projets de texte qu'une loi prévoit, ne saurait être lue comme ne s'appliquant qu'aux seuls avis rendus en application d'une loi spécifique et excluant ainsi les consultations opérées sur le seul fondement de l'article 8 de la loi. Par suite, le décret pourrait très utilement préciser que les avis rendus sur le fondement de la première phrase de l'article 8-I-4^o-a) doivent, eux aussi, faire l'objet d'une publication.

9. De même, la publication des avis sur les projets d'ordonnance relatifs à ces mêmes matières serait utilement prévue. Enfin, la Commission estime que les conditions de publication (modalités exactes, supports, délais, etc.) de l'ensemble des avis de la Commission seraient utilement harmonisées par le projet de décret.

10. **En second lieu**, la Commission souligne l'intérêt s'attachant à ce que le projet de décret lui permette, lorsqu'elle requiert d'un organisme la communication de documents nécessaires à l'exercice de ses missions, d'exiger de ce dernier une version traduite en français de ces documents. En effet, les organismes traitant des données à caractère personnel, et notamment les groupes transnationaux, peuvent disposer de documents en langue étrangère, principalement en anglais, pourtant nécessaires à l'exercice des missions de la Commission, tant en amont de la mise en œuvre d'un traitement (consultation sur une analyse d'impact, outil de transfert de données, etc.) qu'en aval de celle-ci (contrôle sur place ou sur pièces). Or, les dispositions de l'article L. 111-1 du code des relations entre le public et l'administration, relatives à l'usage de la langue française dans les échanges entre l'administration et le public dans le cadre du traitement des demandes de ce dernier, ne semblent pas suffisantes pour exiger une traduction de ces documents si l'organisme en cause n'en dispose pas au moment de la demande faite par la Commission.

11. Une telle possibilité pourrait se fonder sur les dispositions combinées de l'article 18 de la loi du 6 janvier 1978 modifiée, qui disposent que tout organisme traitant des données à caractère personnel doit prendre toutes mesures utiles afin de faciliter la tâche de la Commission, et du deuxième alinéa de l'article 1^{er} de la loi n° 94-665 du 4 août 1994 modifiée relative à l'emploi de la langue française.

12. Afin de ne pas faire porter une charge excessive sur les organismes traitant des données à caractère personnel, une telle disposition pourrait limiter cette faculté d'exiger une traduction aux seuls documents requis par la Commission dont doit en tout état de cause disposer le responsable du traitement ou le sous-traitant en application du Règlement (le registre des activités de traitement, la documentation en matière de violation de données, l'analyse d'impact si celle-ci est nécessaire, etc.).

Sur les dispositions relatives au contrôle de la mise en œuvre des traitements

13. Les dispositions de la section 2 du chapitre Ier du projet de décret, relatives aux modalités de contrôle de la mise en œuvre des traitements, sont largement similaires aux dispositions actuelles du décret du 20 octobre 2005 modifié.

14. Il semble néanmoins nécessaire que toutes les conséquences de la rédaction de l'article 19 de la loi « Informatique et Libertés » soient tirées dans le présent projet de décret concernant l'opposition d'un secret professionnel aux demandes, copies, recueils, accès et transcriptions de documents, renseignements et justifications, programmes informatiques et données en cas de contrôle de la mise en œuvre d'un traitement. Par souci de clarté, l'article 36 du projet de décret, qui mentionne la possibilité d'opposer tout secret professionnel à ces demandes, devrait ainsi être modifié pour rappeler que cette opposabilité ne concerne que les trois secrets limitativement mentionnés à l'article 19 de la loi, à savoir le secret applicable aux relations entre un avocat et son client, le secret des sources des traitements journalistiques et le secret médical, dans les conditions fixées par les mêmes dispositions législatives pour ce dernier.

Sur les dispositions relatives aux mesures correctrices et sanctions

15. Dans l'ensemble, les dispositions relatives aux mesures correctrices et sanctions que peuvent prononcer le président de la Commission et la formation restreinte de cette dernière, en cas de manquement aux dispositions du Règlement et de la loi du 6 janvier 1978 modifiée, tirent toutes les conséquences du nouveau cadre juridique. Elles appellent néanmoins trois séries d'observations.

Sur les astreintes

16. **En premier lieu**, la Commission estime que les dispositions de l'article 43 du projet de décret, relatives aux astreintes qui peuvent assortir les décisions d'injonction de mise en conformité prononcées par la formation restreinte, devraient être complétées sur deux points.

17. Concernant la procédure de liquidation de l'astreinte, il serait tout d'abord utile, à des fins de meilleure lisibilité, de prévoir que les éléments de nature à justifier qu'il s'est conformé à l'injonction, transmis par le responsable du traitement ou le sous-traitant en vertu du deuxième alinéa du même article 43, doivent l'être « *au plus tard à la date fixée par la formation restreinte dans sa décision* ».

18. En outre, la procédure de liquidation de l'astreinte ne faisant intervenir, en l'état du projet de décret, que la seule formation restreinte de la Commission, il peut s'avérer problématique que celle-ci ne dispose pas des attributions lui permettant, le cas échéant, de constater l'inexécution, totale ou partielle, de son injonction, ou son exécution tardive. Des dispositions devraient dès lors être prévues afin de permettre au président de la formation restreinte, au nom de cette dernière, de demander qu'il soit procédé, avec le concours des services de la Commission, à toutes diligences nécessaires aux fins de liquider l'astreinte.

19. A défaut, il conviendrait que le décret prévoie que la décision prononçant la liquidation de l'astreinte peut être précédée d'une procédure écrite au cours de laquelle un rapporteur désigné, à la demande du président de la formation restreinte, dans les conditions prévues à l'article 38 du projet de décret, effectue les diligences utiles et porte à la connaissance de la formation restreinte ainsi que du responsable du traitement ou du sous-traitant les motifs de la liquidation et le montant proposés. Cette phase ne devrait pas intervenir systématiquement, mais seulement dans le cas où le

président de la formation restreinte estime que les éléments spontanément fournis par l'organisme appellent des vérifications complémentaires.

20. De même, la formation restreinte devrait pouvoir auditionner en séance l'organisme concerné lorsque cela est nécessaire, notamment afin de lui permettre de prendre une décision éclairée tenant compte du comportement de l'organisme en cause et des difficultés d'exécution de la décision qu'il a rencontrées.

Sur la coopération européenne

21. **En deuxième lieu**, la Commission estime que deux dispositions de la section 4 du chapitre Ier du projet de décret, relatives aux modalités de coopération de la Commission avec les autorités homologues concernant les mesures correctrices et sanctions qu'elle peut prononcer, devraient être modifiées.

22. Des modifications doivent tout d'abord être apportées aux **dispositions de l'article 51 du projet de décret**, relatives aux conséquences à tirer en cas d'objection des autorités de contrôle concernées à l'égard d'un projet de mise en demeure du président de la Commission, et plus précisément en cas d'objection tendant à ce que soit prononcée une mesure relevant de la compétence de la formation restreinte en lieu et place d'une telle mise en demeure. En l'état, ces dispositions semblent rendre automatique la désignation, par le président de la Commission, d'un rapporteur et, par suite, une décision de la formation restreinte de la Commission, dès lors que de telles objections sont émises par des autorités de contrôle concernées.

23. Or la Commission rappelle que le président de la Commission n'est pas tenu de faire droit à ces objections, qui peuvent en effet être rejetées, et qu'il doit dans ce cas saisir le CEPD en vue d'adopter une décision contraignante, conformément aux dispositions de l'article 65 du RGPD. Cette hypothèse doit dès lors impérativement être réservée par l'article 51 du projet de décret, en complément des dispositions projetées qui ne concernent que le cas où le président de la Commission entend suivre les objections des autorités de contrôle concernées.

24. Cet article devrait également comporter des modalités appropriées d'aménagement du contradictoire dans l'hypothèse où le président de la Commission n'entend pas suivre de telles objections et où il saisit par conséquent le CEPD. En effet, l'adoption d'un projet de mise en demeure du président de la CNIL – qui ne revêt pas le caractère d'une sanction – n'est pas précédée d'une phase contradictoire. Une telle phase n'existe, dans les textes internes, qu'avant le prononcé des mesures de la formation restreinte, qui peuvent revêtir un caractère répressif. Or, ce dualisme des procédures, prévu par le droit français, n'existe pas au niveau européen. Par suite, si le CEPD est saisi, à la suite de de l'objection émise par une autre autorité nationale sur un projet de mise en demeure du président de la Commission, le Comité est susceptible de rendre une décision contraignante qui préempterait en tout ou partie le prononcé, par la suite, d'une mesure par la formation restreinte – si, par exemple, le Comité estimait que les faits justifiaient le prononcé d'une sanction pécuniaire. Dès lors qu'il n'est pas prévu par le Règlement que le CEPD organise lui-même des échanges contradictoires avec les organismes incriminés, la Commission estime que la saisine du Comité devrait, dans ce cas de figure spécifique, être précédée d'une phase contradictoire au niveau français.

25. L'organisme devrait ainsi recevoir, du président de la Commission, toutes les informations utiles relatives à la mise en demeure initialement envisagée et aux objections formulées par les autorités concernées. Il serait ainsi mis à même de présenter ses observations, dans un délai à définir, tant sur le projet initial que sur sa possible « aggravation » par le CEPD. Ses observations seraient ensuite transmises au Comité lors de sa saisine par le président de la Commission.

26. L'article 51 du projet de décret pourrait enfin utilement rappeler la suite de la procédure en cas d'adoption par le CEPD d'une décision contraignante à l'égard de la Commission, en précisant que le président de celle-ci est tenu, en fonction de ce que cette décision implique, soit de prononcer lui-même la mise en demeure, soit de saisir la formation restreinte si la décision contraignante du CEPD impliquait, au vu de la répartition des compétences choisie par le législateur français, que soit prononcée une mesure relevant de la compétence exclusive de la formation restreinte.

27. Des modifications de trois ordres doivent en outre être apportées aux **dispositions de l'article 54 du projet de décret**, relatives aux conséquences à tirer en cas d'objection des autorités de contrôle concernées à l'égard d'un projet de décision de la formation restreinte de la Commission.

28. Tout d'abord, de même que les objections précitées à l'égard du projet de mise en demeure, ces objections peuvent être rejetées par la formation restreinte, qui doit alors saisir le CEPD. Cette hypothèse doit impérativement être rappelée à l'article 54 du projet de décret, étant précisé que cette saisine est indépendante de la nature de l'écart entre le projet de décision de la formation restreinte et la nature des objections des homologues : elle est rendue obligatoire par le RGPD dès lors que cette formation souhaite rejeter ces objections, que celles-ci aient pour objet la diminution ou l'aggravation du projet de décision.

29. En outre, la Commission estime que la réouverture de l'instruction n'est quant à elle nécessaire, aux fins d'assurer les droits de la défense, qu'en cas d'objection tendant à s'écarter du projet de décision dans un sens défavorable à l'organisme mis en cause, et non dans les autres cas de figure, par exemple lorsque la coopération européenne conduit à un adoucissement de la mesure envisagée. Autrement dit, les droits de la défense ne sauraient imposer systématiquement une réouverture de l'instruction. L'article 54 du projet de décret serait donc utilement précisé sur ce point.

30. Enfin, dans le cas où les droits de la défense exigent la réouverture de l'instruction, des modalités significativement allégées de mise en œuvre du contradictoire devraient être prévues. En effet, la formation restreinte doit uniquement, pour se prononcer dans des conditions conformes aux droits de la défense, connaître le point de vue de l'organisme mis en cause face aux objections tendant à s'écarter de la décision proposée initialement dans un sens qui lui est défavorable. Le seul enjeu du contradictoire, à ce stade, est le différentiel entre la proposition initiale, d'une part, et la décision la plus grave susceptible de résulter de la coopération européenne, d'autre part. Les autres aspects de la procédure ont, en revanche, déjà fait l'objet d'un contradictoire complet. De même, en cas de saisine du CEPD, celui-ci ne doit disposer que du projet de décision initial, des objections des autorités de contrôle concernées et des réponses de l'organisme à ces dernières pour se prononcer.

31. Dans les deux cas, la nécessaire défense de l'organisme n'impose aucunement la mise en œuvre d'une procédure aussi longue et itérative que celle prévue aux articles 39 et suivants du projet de décret, sauf à prolonger de manière déraisonnable la procédure. Des modalités assouplies de mise en œuvre du contradictoire doivent dès lors impérativement être prévues à l'article 54 du projet de décret, par exemple en permettant au responsable de traitement ou au sous-traitant de disposer d'un délai de quinze jours, renouvelable une fois si besoin, pour adresser ses observations écrites sur ces objections.

Sur la rédaction projetée de certaines autres dispositions

32. **En troisième lieu**, les dispositions du projet de décret relatives aux mesures correctrices et sanctions appellent les deux remarques suivantes.

33. Le terme de « décision » devrait être préféré à la formule « décision de sanction » à l'article 42 du projet de décret, afin d'inclure l'ensemble des décisions que peut adopter la formation restreinte de la Commission, et notamment les mesures correctrices ne constituant pas des sanctions au sens strict du terme ainsi que les décisions de cette formation ne prononçant ni mesure correctrice ni sanction.

34. L'article 39 du projet de décret devrait par ailleurs être corrigé d'une erreur matérielle au cinquième alinéa, qui renvoie uniquement aux délais prévus aux deuxième et troisième alinéas, excluant ainsi la prolongation des délais nouvellement prévue au quatrième alinéa. Par suite, les articles 45 et 57 du projet de décret, qui renvoient à l'ensemble de ces délais, devraient également être modifiés sur ce point.

Sur les droits des personnes dans le champ d'application du RGPD

35. **En premier lieu**, la Commission relève que les dispositions de l'article 78 du projet de décret relatives aux demandes d'exercice d'un droit présentées par une personne spécialement mandatée à cet effet semblent, à la lettre, être réservées à l'exercice d'un droit sur place, à l'exclusion des autres modalités d'exercice des droits des personnes – en pratique bien plus fréquentes (exercice par formulaire, par courriel, etc.).

36. La Commission s'interroge sur un tel cantonnement. En effet, le recours à de tels mandats est de nature à favoriser l'exercice des droits des personnes concernées, et notamment des personnes placées dans des situations particulières (personnes vulnérables ou peu au fait des pratiques numériques, par exemple), et ne devrait dès lors pas concerner uniquement l'exercice sur place de ces droits. En outre, ce cantonnement n'est pas commandé par le Règlement : le mandat en vue de l'exercice d'un droit auprès du responsable du traitement n'est pas expressément prévu par le RGPD, sans que ce dernier semble pour autant s'y opposer.

37. Par ailleurs, la Commission constate que certaines sociétés spécialisées dans la « récupération » de données recourent déjà largement à de tels mandats pour obtenir la communication de données à caractère personnel, au nom des personnes concernées, auprès de responsables du traitement et que ces demandes suscitent des interrogations de ces derniers.

38. Pour ces raisons, la Commission estime que le projet de décret pourrait utilement être modifié afin, soit de prévoir expressément de tels mandats aux fins de l'exercice de l'ensemble des droits des personnes, quelles qu'en soient les modalités exactes, soit de supprimer toute disposition pouvant être interprétée *a contrario* comme interdisant le recours à ces mandats en-dehors du cas prévu à l'article 78 du projet de décret. Dans la première hypothèse, il conviendrait en outre d'encadrer cette pratique afin d'en sécuriser l'exercice, en prévoyant des conditions supplémentaires à celles qui figurent actuellement audit article (ainsi qu'à l'article 136 du projet de décret s'agissant des traitements relevant du champ d'application de la Directive), telles que l'objet exact du mandat ou la limitation de sa durée.

39. **En deuxième lieu**, la Commission demande que la notion de « demande imprécise » d'exercice d'un droit soit supprimée de l'article 79 du projet de décret. En effet, cette notion ne figure pas dans le Règlement et ces dispositions pourraient permettre aux responsables du traitement de ne pas donner suite, en violation de leurs obligations, aux demandes des personnes concernées pour des motifs vagues et indéterminés. Il convient dès lors de limiter les demandes d'informations complémentaires de ces responsables aux seuls cas, d'une part, de doutes raisonnables quant à l'identité du demandeur, prévu par l'article 12 du RGPD, et, d'autre part, de demande ne comportant pas les éléments permettant d'y répondre, à l'instar de ce que prévoit l'article 143 du projet de décret concernant les demandes que peut faire la CNIL saisie d'une demande d'exercice indirect d'un droit. Les mêmes modifications devraient être apportées aux dispositions des articles 136, concernant les traitements relevant du champ d'application de la Directive, et 147 du projet de décret, concernant les traitements intéressant la sûreté de l'Etat et la défense.

40. **En troisième lieu**, la Commission relève que l'article 82 du projet de décret maintient en droit national des obligations en matière de rectification de données à caractère personnel expressément prévues par l'article 19 du Règlement, alors même que des obligations similaires ne sont pas rappelées concernant d'autres droits des personnes que le droit de rectification. Ces dispositions devraient dès lors être supprimées.

Sur les traitements de données dans le domaine de la santé

41. Les dispositions de la section 2 du chapitre III du Titre II du projet de décret n'appellent que les trois seules observations suivantes.

42. **En premier lieu**, la Commission relève que les dispositions de l'article 94 du projet de décret imposent que la saisine de l'Institut national des données de santé (INDS), pour qu'il se prononce sur le caractère d'intérêt public que présente une recherche, une étude ou une évaluation, soit faite par « la commission » ou le ministre chargé de la santé. L'intervention de la formation plénière de la Commission n'apparaissant ni nécessaire ni proportionnée dans ce cadre, elle demande que cette saisine puisse être faite par le président de la Commission et que le projet de décret, qui a notamment pour objet, conformément aux dispositions du deuxième alinéa de l'article 72 de la loi du 6 janvier 1978 modifiée, de définir les conditions de saisine de l'INDS, soit dès lors modifié sur ce point. En outre, elle souhaite que cette attribution du président de la Commission puisse faire l'objet d'une délégation de signature dans les conditions prévues par le I de l'article 2 du projet de décret et que ces dispositions soient dès lors complétées en ce sens.

43. **En deuxième lieu**, l'article 114 du projet de décret prévoit une information individuelle des personnes accueillies en établissement ou centre « où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement de données à caractère personnel dans le domaine de la santé », en application des dispositions de l'article 69 de la loi du 6 janvier 1978 modifiée. A cet égard, la Commission rappelle que ces dispositions législatives ne sont applicables qu'aux traitements relevant des articles 64 et suivants de la loi précitée, et non à l'ensemble des traitements de données dans le domaine de la santé. En particulier, en sont exclus, en vertu du 1° de l'article 65, les traitements mentionnés au 1° de l'article 44 de la même loi, qui comprennent notamment les traitements « nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé ». Dès lors, ce n'est que dans le cas où de tels traitements relèveraient effectivement des dispositions des articles 64 et suivants de la loi « Informatique et Libertés », par exemple les traitements mis en œuvre à des fins de recherche par ces établissements ou centres, et non dans le cas où ils se limiteraient à une prise en charge médicale, que cette information individuelle devrait être requise.

44. **En troisième lieu**, des erreurs matérielles du projet de décret devraient être corrigées. L'article 112 du projet de décret devrait ainsi faire référence à l'article 110 du même texte pour désigner les référentiels, règlements type et méthodologies de référence, et non à l'article 109. La référence à des « prélèvements biologiques identifiants » à l'article 116 du projet de décret devrait être remplacée par « l'examen des caractéristiques génétiques », afin de prendre acte des modifications législatives intervenues sur ce point.

Sur les autres obligations incombant aux responsables du traitement et aux sous-traitants

45. Le projet de décret ne rappelle pas l'ensemble des obligations incombant à ces organismes en application directe du Règlement, et notamment l'obligation de notification auprès de la Commission de toute violation de données, prévue par l'article 33 du RGPD. Si ces obligations auraient pu utilement être rappelées par renvoi aux dispositions applicables du Règlement, à l'instar de ce que prévoit la loi du 6 janvier 1978 modifiée en ce qui concerne les droits des personnes, la Commission estime en tout état de cause que deux dispositions procédurales devraient être prévues concernant ces notifications, distinctes de celles prévues au chapitre IV du Titre II du projet de décret, qui ne concerne que le secteur des communication électroniques.

46. L'obligation de notification de la Commission par voie électronique, déjà prévue à l'article 61 du projet de décret pour les déclarations, consultations et demandes d'avis et d'autorisation émanant d'usagers professionnels et à laquelle il est déjà en pratique largement recouru, serait ainsi utilement prévue par le projet de décret. En outre, ce dernier devrait préciser que le silence de la Commission dans un délai de deux mois vaut décision de l'absence de nécessité de communiquer la violation aux personnes concernées au sens de l'article 34.4 du Règlement.

Sur les dispositions régissant les traitements de données relatives aux personnes décédées

47. La Commission estime que le second alinéa de l'article 125 du projet de décret n'est pas conforme aux dispositions de la loi « Informatique et Libertés » concernant ces traitements. L'article 84 de ladite loi prévoit en effet que les traitements de données relatives aux personnes décédées sont régis par les seules dispositions du chapitre V de la loi du 6 janvier 1978 modifiée et précise notamment que les droits des personnes concernées s'éteignent à leur décès. Le projet de décret, en prévoyant que les droits et obligations mentionnés au titre II du décret, relatif aux traitements relevant du champ d'application du Règlement, s'appliquent aux traitements de données de personnes décédées, fait donc une inexacte application des dispositions législatives précitées.

Sur les transferts de données vers les Etats n'appartenant pas à l'Union européenne

48. La Commission estime que le chapitre VI du titre II du projet de décret, relatif aux transferts de données, devrait être complété de nouvelles dispositions concernant les arrangements administratifs mentionnés à l'article 46 du Règlement. Conformément à ces dispositions, de tels arrangements doivent prévoir des « *droits opposables et effectifs* » pour les personnes concernées pour constituer des garanties appropriées permettant de transférer des données vers un pays tiers. Dans la mesure où une telle opposabilité vis-à-vis des personnes physiques concernées ne peut être assurée que par l'intermédiaire d'une publication de ces arrangements, le cas échéant selon des modalités adaptées, la Commission estime que le projet de décret devrait prévoir le principe d'une telle publication, qui pourrait intervenir sur le site de la Commission ou de l'organisme national concerné.

Sur les dispositions applicables aux traitements relevant de la Directive et aux traitements intéressant la sécurité publique, la sûreté de l'Etat ou la défense

49. Les dispositions des titres III et IV du projet de décret, concernant respectivement les traitements relevant du champ d'application de la Directive et les traitements ne relevant pas du droit de l'Union, sont en substance inchangées par rapport aux dispositions actuellement en vigueur en vertu du décret du 20 octobre 2005 modifié. Elles appellent néanmoins les observations suivantes.

Sur la possibilité d'une analyse d'impact commune dans le champ de la Directive

50. La Commission relève tout d'abord que le projet de décret ne prévoit pas la possibilité de procéder à une analyse d'impact relative à la protection des données à caractère personnel (AIPD) commune à plusieurs traitements similaires relevant de la Directive et susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes.

51. Si cette possibilité n'est pas expressément prévue par la Directive, contrairement à ce qui est prévu par le Règlement pour les traitements similaires présentant des risques élevés, la Commission estime qu'une disposition autorisant une telle analyse commune ne serait pas incompatible avec le texte européen. Au contraire, dans la mesure où elle établit un socle de référence des garanties minimales à mettre en œuvre par l'ensemble

des responsables du traitement concernés, elle pourrait constituer une modalité appropriée de transposition de la Directive à certaines catégories de traitements, appelés à être déployés à une large échelle sans adaptation substantielle de leurs caractéristiques propres (hors mesures de sécurité). Elle pourrait également constituer, au niveau national, une « garantie plus étendue » pour la protection des droits et des libertés des personnes au sens de l'article 1^{er} de la Directive.

52. En outre, la singularité du droit national quant aux traitements relevant de la Directive, qui prévoit notamment que ceux-ci peuvent être autorisés par un acte réglementaire unique au sens du IV de l'article 31 de la loi du 6 janvier 1978 modifiée dès lors qu'ils répondent à des finalités et des modalités de mise en œuvre identiques, justifie que ces mêmes traitements puissent faire l'objet d'une AIPD commune comportant un socle minimal de mesures à mettre en œuvre par chaque responsable de traitement concerné. Elle permettrait ainsi de faciliter la mise en œuvre de certains traitements tout en garantissant un contrôle adapté à leurs spécificités.

53. Compte tenu des considérations de bonne administration précitées, la Commission estime dès lors souhaitable que le projet de décret, sans méconnaître les dispositions de l'article 90 de la loi du 6 janvier 1978 modifiée qui prévoient que l'analyse d'impact est effectuée par le responsable de traitement, ouvre la faculté d'établir, par le biais d'une analyse d'impact commune ou d'un référentiel général pouvant être complété dans l'élaboration de l'AIPD en fonction des spécificités de chaque traitement, un tel socle commun de garanties minimales.

Sur la communication à la Commission des analyses d'impact relatives à certains traitements

54. Les analyses d'impact peuvent concerner, non seulement les traitements relevant de la Directive, mais également certains traitements relevant du Règlement et soumis à formalité préalable auprès de la Commission, comme par exemple certains traitements intéressant la sécurité publique. Si l'article 90 de la loi « Informatique et Libertés » le prévoit expressément s'agissant des traitements relevant de la Directive, la Commission estime que l'article 66 du projet de décret devrait, pour la seconde catégorie de traitements, prévoir l'obligation d'adresser cette analyse d'impact, si celle-ci est nécessaire en application des dispositions du RGPD, à l'appui de la demande d'avis auprès de la Commission. Il pourrait également rappeler cette obligation prévue par la loi s'agissant des traitements relevant de la Directive.

55. Il est en effet impératif de disposer d'une telle analyse d'impact pour rendre un avis éclairé sur le traitement envisagé, sauf à compromettre le bon examen de cette demande d'avis. A cet égard, la Commission estime que les dispositions de l'article 33 de la loi du 6 janvier 1978 modifiée, qui établissent les éléments devant, en toutes circonstances, être communiqués à la Commission à l'occasion d'une demande d'avis, ne sauraient être interprétées comme excluant la possibilité de prévoir, par voie réglementaire, des éléments supplémentaires à fournir à la Commission dans certains cas particuliers. Enfin, elle rappelle que les délais d'examen de la demande d'avis, encadrés par la loi du 6 janvier 1978, ont précisément été modifiés par l'ordonnance précitée du 12 décembre 2018 pour correspondre aux délais d'examen des AIPD pour lesquelles une consultation de la Commission est obligatoire. Au vu de ces éléments, la Commission demande que l'article 66 du projet de décret soit complété sur ce point.

56. En outre, elle estime utile de prévoir la possibilité qu'une telle analyse puisse également être jointe à l'engagement de conformité à un acte réglementaire unique, prévu à l'article 67 du même projet. Une telle précision permettrait de compléter utilement les dispositions de la loi du 6 janvier 1978 modifiée qui n'ont pas, par définition, vocation à régir tous les cas de figure.

57. En effet, le deuxième alinéa de l'article 90 de la loi du 6 janvier 1978 modifiée prévoit une obligation de transmission de l'AIPD à la Commission à l'appui de la demande d'avis pour les traitements relevant de la Directive et mis en œuvre pour le compte de l'Etat. Le troisième alinéa du même article prévoit la consultation de la Commission sur une telle AIPD lorsque le traitement n'est pas mis en œuvre pour le compte de l'Etat, dans la mesure où cette analyse d'impact ne peut alors s'adosser à une demande d'avis auprès de la CNIL. Ainsi, les dispositions législatives ne prévoient pas les cas des traitements relevant de la Directive mis en œuvre pour le compte de l'Etat et encadrés par un acte réglementaire unique, qui ne font dès lors pas l'objet d'une demande d'avis spécifique, ainsi que des traitements relevant du Règlement et faisant de même l'objet d'un tel acte réglementaire unique. Pour ces traitements qui présentent des risques élevés, dans la mesure où ils sont soumis à analyse d'impact préalable, il serait cohérent que la Commission dispose également, tout comme pour les autres traitements précités, de l'AIPD effectuée par le responsable de traitement.

58. Enfin et en tout état de cause, s'agissant de l'analyse d'impact mentionnée à l'article 131 du projet de décret, qui concerne uniquement les traitements relevant de la Directive, la Commission rappelle qu'elle doit fournir un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant dans le cas où elle estime que le traitement constituerait une violation des dispositions des titres Ier et III de la loi du 6 janvier 1978 modifiée, et non de son seul titre III. Par exemple, les manquements aux principes relatifs au traitement de données (finalité, pertinence, durée de conservation appropriée, etc.), établis au sein du Titre Ier de la loi précitée et applicables aux traitements relevant de la Directive, peuvent en effet naturellement justifier l'adoption d'un tel avis par la formation plénière de la Commission. Le quatrième alinéa de l'article 131 du projet de décret doit dès lors être modifié sur ce point.

Sur les droits des personnes concernées

59. S'agissant des droits des personnes, et outre les observations déjà formulées concernant le mandat, pour les seuls traitements relevant de la Directive, et la notion de demande imprécise, pour les mêmes traitements ainsi que ceux intéressant la sûreté de l'Etat et la défense, la Commission estime que la lisibilité du titre IV du projet de décret devrait être améliorée. Il convient en effet de mieux distinguer, par exemple en créant deux sous-sections distinctes, les dispositions applicables aux traitements pour lesquels les demandes d'exercice d'un droit ne peuvent être réalisées que de manière indirecte, par l'intermédiaire de la Commission, ce qui représente en pratique l'immense majorité des cas, des dispositions applicables aux traitements pour lesquels aucune restriction des droits, y compris l'exercice indirect de ces droits, n'est prévue.

60. Enfin, il serait utile de clarifier la rédaction du dernier alinéa de l'article 144 du projet de décret, relatif à la mention, par la Commission, des voies et délais de recours ouverts aux personnes concernées par les traitements intéressant la sûreté de l'Etat. La rédaction actuelle conduit en effet à reprendre *in extenso* les dispositions de l'article R. 841-2 du code de la sécurité intérieure dans les courriers de notification adressés

aux demandeurs, alors même que la référence auxdites dispositions pourrait être formulée dans un langage plus compréhensible pour ces personnes.

La Présidente



Marie-Laure DENIS