TEXTE ADOPTÉ n° **113**
« Petite loi »

—

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

SESSION ORDINAIRE DE 2017-2018

14 mai 2018

PROJET DE LOI

relatif à la **protection** *des* **données personnelles**.

(Texte définitif)

L'Assemblée nationale a adopté, dans les conditions prévues à l'article 45, alinéa 4, de la Constitution, le projet de loi dont la teneur suit :

Voir les numéros :

Assemblée nationale : 1re lecture : **490**, **592**, **579** et T.A. **84**.
Commission mixte paritaire : **855**.
Nouvelle lecture : **809**, **860** et T.A. **110**.
Lecture définitive : **903**.

Sénat : 1re lecture : **296**, **350**, **351** et T.A. **76** (2017-2018).
Commission mixte paritaire : **407** et **408** (2017-2018).
Nouvelle lecture : **425**, **441**, **442** et T.A. **100** (2017-2018).

.....

TITRE I^ER

DISPOSITIONS D'ADAPTATION COMMUNES AU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016 ET À LA DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016

CHAPITRE I^ER

Dispositions relatives à la Commission nationale de l'informatique et des libertés

Article 1^er

L'article 11 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié :

1° Au début du premier alinéa, est ajoutée la mention : « I. – » ;

2° Après la première phrase du même premier alinéa, est insérée une phrase ainsi rédigée : « Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité » ;

3° Le 1° est complété par les mots : « et peut, à cette fin, apporter une information adaptée aux collectivités territoriales, à leurs groupements et aux petites et moyennes entreprises » ;

4° Le 2° est ainsi modifié :

a) Le premier alinéa est complété par les mots : « et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France » ;

b) Au *a*, les mots : « autorise les traitements mentionnés à l'article 25, » et, à la fin, les mots : « et reçoit les déclarations relatives aux autres traitements » sont supprimés ;

c) Après le même *a*, il est inséré un *a* bis ainsi rédigé :

« *a* bis*)* Elle établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle prend en compte la situation des personnes dépourvues de compétences numériques. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables de traitement et à leurs sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques, notamment des mineurs, et des besoins spécifiques des collectivités territoriales, de leurs groupements et des micro-entreprises, petites entreprises et moyennes entreprises ; elle homologue et publie les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel ; »

d) Le *b* est ainsi rédigé :

« *b)* En concertation avec les organismes publics et privés représentatifs des acteurs concernés, elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé. À ce titre, sauf pour les traitements mis en œuvre pour le compte de l'État agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures, notamment techniques et organisationnelles, supplémentaires pour le traitement des données biométriques, génétiques et de santé en application du 4 de l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et des garanties complémentaires en matière de traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions conformément à l'article 10 du même règlement ; »

e) Après le *f*, il est inséré un *f* bis ainsi rédigé :

« *f* bis*)* Elle peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et à la présente loi. Elle prend en considération, à cette fin, les besoins spécifiques des collectivités territoriales, de leurs groupements et des micro-entreprises, petites entreprises et moyennes entreprises. Elle agrée, aux mêmes fins, des organismes certificateurs, sur la base, le cas échéant, de leur accréditation par l'organisme national d'accréditation mentionné au *b* du 1 de l'article 43 du même règlement ou

décide, conjointement avec cet organisme, que ce dernier procède à leur agrément, dans des conditions précisées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. La commission élabore ou approuve les critères des référentiels de certification et d'agrément ; »

f) Au *g*, après le mot : « certification », sont insérés les mots : « , par des tiers agréés ou accrédités selon les modalités mentionnées au *f* bis du présent 2°, » ;

g) À la fin du *h*, les mots : « d'accès concernant les traitements mentionnés aux articles 41 et 42 » sont remplacés par les mots : « ou saisines prévues aux articles 41, 42 et 70-22 » ;

h) Sont ajoutés des *i* et *j* ainsi rédigés :

« *i)* Elle peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable conformément à l'article 70-4 ;

« *j)* Elle mène des actions de sensibilisation auprès des médiateurs de la consommation et des médiateurs publics, au sens de l'article L. 611-1 du code de la consommation, en vue de la bonne application de la présente loi ; »

5° Après la première phrase du *a* du 4°, est insérée une phrase ainsi rédigée : « Elle peut également être consultée par le Président de l'Assemblée nationale, par le Président du Sénat ou par les commissions compétentes de l'Assemblée nationale et du Sénat ainsi qu'à la demande d'un président de groupe parlementaire sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données. » ;

6° Après le même 4°, il est inséré un 5° ainsi rédigé :

« 5° Elle peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application de la présente loi et des dispositions relatives à la protection des données personnelles prévues par les textes législatifs et règlementaires, le droit de l'Union européenne, y compris le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, et les engagements internationaux de la France. » ;

7° Au début du vingt-sixième alinéa, est ajoutée la mention : « II. – » ;

8° L'avant-dernier alinéa est supprimé.

Article 2

Le I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au 6°, le mot : « ou » est remplacé par le mot : « et » ;

2° Au 7°, après le mot : « numérique », sont insérés les mots : « et des questions touchant aux libertés individuelles ».

Article 3

L'article 15 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Après le premier alinéa, il est inséré un alinéa ainsi rédigé :

« L'ordre du jour de la commission réunie en formation plénière est rendu public. » ;

2° Sont ajoutés trois alinéas ainsi rédigés :

« – au 4 de l'article 34 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, pour les décisions donnant acte du respect des conditions mentionnées au 3 du même article 34 ;

« – aux *a* et *h* du 3 de l'article 58 du même règlement.

« Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les conditions et limites dans lesquelles le président de la commission et le vice-président délégué peuvent déléguer leur signature. »

Article 4

La loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifiée :

1° Au premier alinéa de l'article 17, après le mot : « restreinte », sont insérés les mots : « prend les mesures et », après le mot : « traitements », sont insérés les mots : « ou des sous-traitants » et, après le mot : « découlant », sont insérés les mots : « du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et » ;

2° Après le même premier alinéa, il est inséré un alinéa ainsi rédigé :

« Ses membres délibèrent hors de la présence des agents de la commission, à l'exception de ceux chargés de la tenue de la séance. » ;

3° Les deux derniers alinéas de l'article 18 sont ainsi rédigés :

« Le commissaire du Gouvernement assiste à toutes les délibérations de la commission réunie en formation plénière ainsi qu'à celles des réunions de son bureau qui ont pour objet l'exercice des attributions déléguées en application de l'article 16. Il peut assister aux séances de la formation restreinte, sans être présent au délibéré. Il est rendu destinataire de l'ensemble des avis et décisions de la commission et de la formation restreinte.

« Sauf en matière de mesures ou de sanctions relevant du chapitre VII, il peut provoquer une seconde délibération de la commission, qui doit intervenir dans les dix jours suivant la délibération initiale. »

Article 5

L'article 44 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au premier alinéa du I, les mots : « et qui sont à usage professionnel » sont supprimés ;

2° Le II est ainsi modifié :

a) À la première phrase du premier alinéa, les mots : « de locaux professionnels privés » sont remplacés par les mots : « de ces lieux, locaux, enceintes, installations ou établissements » ;

b) La dernière phrase du dernier alinéa est complétée par les mots : « dont la finalité est l'exercice effectif des missions prévues au III » ;

3° Les trois premiers alinéas du III sont remplacés par deux alinéas ainsi rédigés :

« III. – Pour l'exercice des missions relevant de la Commission nationale de l'informatique et des libertés en application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et de la présente loi, les membres et agents mentionnés au premier alinéa du I du présent article peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission. Ils peuvent accéder, dans des conditions

préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve du deuxième alinéa du présent III, par le secret médical.

« Le secret médical est opposable s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé. La communication des données médicales individuelles incluses dans cette catégorie de traitement ne peut alors se faire que sous l'autorité et en présence d'un médecin. » ;

4° Avant le dernier alinéa du même III, sont insérés deux alinéas ainsi rédigés :

« Pour le contrôle de services de communication au public en ligne, les membres et agents mentionnés au premier alinéa du I peuvent réaliser toute opération en ligne nécessaire à leur mission sous une identité d'emprunt. À peine de nullité, leurs actes ne peuvent constituer une incitation à commettre une infraction. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées conformément au troisième alinéa du présent III. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, précise les conditions dans lesquelles ces membres et agents procèdent dans ces cas à leurs constatations.

« Les membres et agents mentionnés au premier alinéa du I peuvent, à la demande du président de la commission, être assistés par des experts. » ;

5° Il est ajouté un V ainsi rédigé :

« V. – Dans l'exercice de son pouvoir de contrôle portant sur les traitements relevant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et de la présente loi, la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions. »

Article 6

La loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifiée :

1° Après l'article 48, il est inséré un chapitre VII *bis*, intitulé : « De la coopération » et comprenant les articles 49 à 49-5 tels qu'ils résultent des 2° à 4° du présent article ;

2° L'article 49 est ainsi rédigé :

« *Art. 49.* – Dans les conditions prévues aux articles 60 à 67 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, la Commission nationale de l'informatique et des libertés met en œuvre des procédures de coopération et d'assistance mutuelle avec les autorités de contrôle des autres États membres de l'Union européenne et réalise avec ces autorités des opérations conjointes.

« La commission, le président, le bureau, la formation restreinte et les agents de la commission mettent en œuvre, chacun pour ce qui le concerne, les procédures mentionnées au premier alinéa du présent article.

« La commission peut charger le bureau :

« 1° D'exercer ses prérogatives en tant qu'autorité concernée, au sens du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, et en particulier d'émettre une objection pertinente et motivée au projet de décision d'une autre autorité de contrôle ;

« 2° Lorsque la commission adopte un projet de décision en tant qu'autorité chef de file ou autorité compétente, de mettre en œuvre les procédures de coopération, de contrôle de la cohérence et de règlement des litiges prévues par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et d'arrêter la décision au nom de la commission. » ;

3° Après le même article 49, sont insérés des articles 49-1 à 49-4 ainsi rédigés :

« *Art. 49-1.* – I. – Pour l'application de l'article 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, la Commission nationale de l'informatique et des libertés coopère avec les autorités de contrôle des autres États membres de l'Union européenne, dans les conditions prévues au présent article.

« II. – Qu'elle agisse en tant qu'autorité de contrôle chef de file ou en tant qu'autorité concernée au sens des articles 4 et 56 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, la Commission nationale de l'informatique et des libertés est compétente pour traiter une réclamation ou une éventuelle violation des dispositions du même règlement affectant par ailleurs d'autres États membres. Le président de la commission invite les autres autorités de contrôle concernées à participer aux opérations de contrôle conjointes qu'il décide de conduire.

« III. – Lorsqu'une opération de contrôle conjointe se déroule sur le territoire français, des membres ou agents habilités de la commission, agissant en tant qu'autorité de contrôle d'accueil, sont présents aux côtés des membres et agents des autres autorités de contrôle participant, le cas échéant, à l'opération. À la demande de l'autorité de contrôle d'un État membre, le président de la commission peut 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 commission, en application de l'article 19 de la présente loi, à exercer, sous son autorité, tout ou partie des pouvoirs de vérification et d'enquête dont disposent les membres et les agents de la commission.

« IV. – Lorsque la commission est invitée à contribuer à une opération de contrôle conjointe décidée par l'autorité de contrôle d'un autre État membre, le président de la commission se prononce sur le principe et les conditions de la participation, désigne les membres et agents habilités et en informe l'autorité requérante dans les conditions prévues à l'article 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

« *Art. 49-2*. – I. – Les traitements mentionnés à l'article 70-1 font l'objet d'une coopération entre la Commission nationale de l'informatique et des libertés et les autorités de contrôle des autres États membres de l'Union européenne dans les conditions prévues au présent article.

« II. – La commission communique aux autorités de contrôle des autres États membres les informations utiles et leur prête assistance en mettant notamment en œuvre, à leur demande, des mesures de contrôle telles que des mesures de consultation, d'inspection et d'enquête.

« La commission répond à une demande d'assistance mutuelle formulée par une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande contenant toutes les informations

nécessaires, notamment sa finalité et ses motifs. Elle ne peut refuser de satisfaire à cette demande que si elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter, ou si une disposition du droit de l'Union européenne ou du droit français y fait obstacle.

« La commission informe l'autorité de contrôle requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande.

« La commission peut, pour l'exercice de ses missions, solliciter l'assistance d'une autorité de contrôle d'un autre État membre de l'Union européenne.

« La commission donne les motifs de tout refus de satisfaire à une demande lorsqu'elle estime ne pas être compétente ou lorsqu'elle considère que satisfaire à la demande constituerait une violation du droit de l'Union européenne ou du droit français.

« *Art. 49-3*. – Lorsque la commission agit en tant qu'autorité de contrôle chef de file s'agissant d'un traitement transfrontalier au sein de l'Union européenne, elle communique sans tarder aux autres autorités de contrôle concernées le rapport du rapporteur mentionné au premier alinéa de l'article 47 ainsi que l'ensemble des informations utiles de la procédure ayant permis d'établir le rapport, avant l'éventuelle audition du responsable de traitement ou de son sous-traitant. Les autorités concernées sont mises en mesure d'assister, par tout moyen de retransmission approprié, à l'audition par la formation restreinte du responsable de traitement ou de son sous-traitant, ou de prendre connaissance d'un procès-verbal dressé à la suite de l'audition.

« Après en avoir délibéré, la formation restreinte soumet son projet de décision aux autres autorités de contrôle concernées conformément à la procédure définie à l'article 60 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité. À ce titre, elle se prononce sur la prise en compte des objections pertinentes et motivées émises par ces autorités et saisit, si elle décide d'écarter l'une des objections, le comité européen de la protection des données conformément à l'article 65 du même règlement.

« Les conditions d'application du présent article sont définies par décret en Conseil d'État, après avis de la Commission nationale de l'informatique et des libertés.

« *Art. 49-4*. – Lorsque la commission agit en tant qu'autorité de contrôle concernée, au sens du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, le président de la commission est saisi des projets de mesures correctrices soumis à la commission par une autorité de contrôle chef de file.

« Lorsque ces mesures sont d'objet équivalent à celles définies aux I et II de l'article 45 de la présente loi, le président décide, le cas échéant, d'émettre une objection pertinente et motivée, selon les modalités prévues à l'article 60 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

« Lorsque ces mesures sont d'objet équivalent à celles définies au III de l'article 45 de la présente loi, le président saisit la formation restreinte. Le président de la formation restreinte ou le membre de la formation restreinte qu'il désigne peut, le cas échéant, émettre une objection pertinente et motivée selon les mêmes modalités. » ;

4° L'article 49 *bis* devient l'article 49-5.

Article 7

I. – Le chapitre VII de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° L'intitulé est ainsi rédigé : « Mesures et sanctions prises par la formation restreinte de la Commission nationale de l'informatique et des libertés » ;

2° Les articles 45 à 48 sont ainsi rédigés :

« *Art. 45*. – I. – Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable de traitement ou son sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi.

« II. – Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, si le manquement constaté est susceptible de faire l'objet

d’une mise en conformité, prononcer à son égard une mise en demeure, dans le délai qu’il fixe :

« 1° De satisfaire aux demandes présentées par la personne concernée en vue d’exercer ses droits ;

« 2° De mettre les opérations de traitement en conformité avec les dispositions applicables ;

« 3° À l’exception des traitements qui intéressent la sûreté de l’État ou la défense, de communiquer à la personne concernée une violation de données à caractère personnel ;

« 4° De rectifier ou d’effacer des données à caractère personnel, ou de limiter le traitement de ces données.

« Dans le cas prévu au 4° du présent II, le président peut, dans les mêmes conditions, mettre en demeure le responsable de traitement ou son sous-traitant de notifier aux destinataires des données les mesures qu’il a prises.

« Le délai de mise en conformité peut être fixé à vingt-quatre heures en cas d’extrême urgence.

« Le président prononce, le cas échéant, la clôture de la procédure de mise en demeure.

« Le président peut demander au bureau de rendre publique la mise en demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l’objet de la même publicité.

« III. – Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l’informatique et des libertés peut également, le cas échéant après lui avoir adressé l’avertissement prévu au I du présent article ou, le cas échéant en complément d’une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l’une ou de plusieurs des mesures suivantes :

« 1° Un rappel à l’ordre ;

« 2° Une injonction de mettre en conformité le traitement avec les obligations résultant de la présente loi ou du règlement (UE) 2016/679 du

Parlement européen et du Conseil du 27 avril 2016 précité ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ;

« 3° À l'exception des traitements qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du chapitre XIII de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'État, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du même règlement ou de la présente loi ;

« 4° Le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;

« 5° La suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;

« 6° La suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes ;

« 7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

« Le projet de mesure est, le cas échéant, soumis aux autres autorités de contrôle concernées selon les modalités définies à l'article 60 du même règlement.

« *Art. 46*. – I. – Lorsque le non-respect des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi entraîne une violation des droits et libertés mentionnés à l'article 1er de la présente loi et que le président de la commission considère qu'il est urgent d'intervenir, il saisit la formation restreinte, qui peut, dans le cadre d'une procédure d'urgence contradictoire définie par décret en Conseil d'État, adopter l'une des mesures suivantes :

« 1° L'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du chapitre XIII lorsqu'ils sont mis en œuvre pour le compte de l'État ;

« 2° La limitation du traitement de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du même chapitre XIII lorsqu'ils sont mis en œuvre pour le compte de l'État ;

« 3° La suspension provisoire de la certification délivrée au responsable de traitement ou à son sous-traitant ;

« 4° La suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite ;

« 5° La suspension provisoire de l'autorisation délivrée sur le fondement du III de l'article 54 de la présente loi ;

« 6° L'injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans le cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ;

« 7° Un rappel à l'ordre ;

« 8° L'information du Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du chapitre XIII de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'État. Le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

« II. – En cas de circonstances exceptionnelles prévues au 1 de l'article 66 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, lorsque la formation restreinte adopte les mesures provisoires prévues aux 1° à 4° du I du présent article, elle informe sans délai de la teneur des mesures prises et de leurs motifs les autres

autorités de contrôle concernées, le comité européen de la protection des données et la Commission européenne.

« Lorsque la formation restreinte a pris de telles mesures et qu'elle estime que des mesures définitives doivent être prises, elle met en œuvre les dispositions du 2 de l'article 66 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

« III. – Pour les traitements relevant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, lorsqu'une autorité de contrôle compétente en application du même règlement n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées, la formation restreinte, saisie par le président de la commission, peut demander au comité européen de la protection des données un avis d'urgence ou une décision contraignante d'urgence dans les conditions et selon les modalités prévues aux 3 et 4 de l'article 66 dudit règlement.

« IV. – En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er de la présente loi, le président de la commission peut en outre demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.

« *Art. 47*. – Les mesures prévues au III de l'article 45 et aux 1° à 7° du I de l'article 46 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable de traitement ou à son sous-traitant, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris, à la demande du secrétaire général de la commission, les agents des services de celle-ci.

« La formation restreinte peut rendre publiques les mesures qu'elle prend. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne, aux frais des personnes sanctionnées.

« Sans préjudice des obligations d'information qui incombent au responsable de traitement ou à son sous-traitant en application de l'article 34 du règlement (UE) 2016/679 du Parlement européen et du

Conseil du 27 avril 2016 précité, la formation restreinte peut ordonner que ce responsable ou ce sous-traitant informe individuellement, à ses frais, chacune des personnes concernées de la violation relevée des dispositions de la présente loi ou du règlement précité ainsi que, le cas échéant, de la mesure prononcée.

« Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce.

« L'astreinte est liquidée par la formation restreinte, qui en fixe le montant définitif.

« Les sanctions pécuniaires et les astreintes sont recouvrées comme les créances de l'État étrangères à l'impôt et au domaine.

« *Art. 48*. – Lorsqu'un organisme de certification ou un organisme chargé du respect d'un code de conduite a manqué à ses obligations ou n'a pas respecté les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou celles de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, le cas échéant après mise en demeure, saisir la formation restreinte de la commission, qui peut prononcer, dans les mêmes conditions que celles prévues aux articles 45 à 47, le retrait de l'agrément qui a été délivré à cet organisme. »

II. – A. – Au deuxième alinéa de l'article 226-16 du code pénal, la référence : « I » est remplacée par la référence : « III ».

B. – Le deuxième alinéa de l'article 226-16 du code pénal demeure applicable, dans sa rédaction antérieure à la présente loi, aux faits commis avant l'entrée en vigueur de celle-ci.

CHAPITRE II

Dispositions relatives à certaines catégories de données

Article 8

L'article 8 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Le I est ainsi rédigé :

« I. – Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. » ;

2° Le II est ainsi modifié :

a) À la fin du 7°, les mots : « et dans les conditions prévues à l'article 25 de la présente loi » sont supprimés ;

b) Le 8° est ainsi rédigé :

« 8° Les traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions du chapitre IX de la présente loi ; »

c) Sont ajoutés des 9° à 11° ainsi rédigés :

« 9° Les traitements conformes aux règlements types mentionnés au *b* du 2° du I de l'article 11 mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires ;

« 10° Les traitements portant sur la réutilisation des informations publiques figurant dans les jugements et décisions mentionnés, respectivement, à l'article L. 10 du code de justice administrative et à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que ces traitements n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées ;

« 11° Les traitements nécessaires à la recherche publique au sens de l'article L. 112-1 du code de la recherche, mis en œuvre dans les conditions prévues au 2 de l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, après avis motivé et publié de la Commission nationale de l'informatique et des libertés rendu selon les modalités prévues à l'article 28 de la présente loi. » ;

3° Le III est ainsi rédigé :

« III. – N’entrent pas dans le champ de l’interdiction prévue au I les données à caractère personnel mentionnées au même I qui sont appelées à faire l’objet, à bref délai, d’un procédé d’anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l’informatique et des libertés. » ;

4° Le IV est ainsi rédigé :

« IV. – De même, ne sont pas soumis à l’interdiction prévue au I les traitements, automatisés ou non, justifiés par l’intérêt public et autorisés dans les conditions prévues au II de l’article 26. »

TITRE II

MARGES DE MANŒUVRE PERMISES PAR 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

Article 9

L’article 2 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au premier alinéa, après les mots : « traitements automatisés », sont insérés les mots : « en tout ou partie » ;

2° L’avant-dernier alinéa est complété par les mots : « , que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

CHAPITRE I^ER

Champ d'application territorial des dispositions complétant le règlement (UE) 2016/679

Article 10

Le chapitre I^er de la loi n° 78-17 du 6 janvier 1978 est complété par un article 5-1 ainsi rédigé :

« *Art. 5-1.* – Les règles nationales prises sur le fondement des dispositions du 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 renvoyant au droit national le soin d'adapter ou de compléter les droits et obligations prévus par ce règlement s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France.

« Toutefois, lorsqu'est en cause un des traitements mentionnés au 2 de l'article 85 du même règlement, les règles nationales mentionnées au premier alinéa du présent article sont celles dont relève le responsable de traitement, lorsqu'il est établi dans l'Union européenne. »

CHAPITRE II

Dispositions relatives à la simplification des formalités préalables à la mise en œuvre des traitements

Article 11

I. – L'article 22 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« *Art. 22.* – Un décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, détermine les catégories de responsables de traitement et les finalités de ces traitements au vu desquelles ces derniers peuvent être mis en œuvre lorsqu'ils portent sur des données comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. La mise en œuvre des traitements intervient sans préjudice des obligations

qui incombent aux responsables de traitement ou à leurs sous-traitants en application de la section 3 du chapitre IV du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

« N'entrent pas dans le champ d'application du premier alinéa du présent article ceux des traitements portant sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire :

« 1° Qui ont exclusivement des finalités de statistique publique, sont mis en œuvre par le service statistique public et ne comportent aucune des données mentionnées au I de l'article 8 ou à l'article 9 ;

« 2° Qui ont exclusivement des finalités de recherche scientifique ou historique ;

« 3° Qui ont pour objet de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, mis en œuvre par l'État, une personne morale de droit public ou une personne morale de droit privé gérant un service public.

« Pour les traitements dont les finalités sont mentionnées aux 1° et 2° du présent article, 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 signifiant. Cette opération est renouvelée à une fréquence définie par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. Les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique ne sont pas soumis au premier alinéa.

« Pour les traitements dont les finalités sont mentionnées au 1°, l'utilisation du code statistique non signifiant n'est autorisée qu'au sein du service statistique public.

« Pour les traitements dont les finalités sont mentionnées au 2°, l'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu ne peuvent être assurées par la même personne ni par le responsable de traitement.

« À l'exception des traitements mentionnés au deuxième alinéa de l'article 55, le présent article n'est pas applicable aux traitements de données à caractère personnel dans le domaine de la santé qui sont régis par le chapitre IX. »

II. – L'article 27 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« *Art. 27*. – Sont autorisés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. »

III. – Les articles 23 à 25 de la loi n° 78-17 du 6 janvier 1978 précitée sont abrogés.

IV. – L'article 226-16-1 A du code pénal est abrogé.

CHAPITRE III

Obligations incombant aux responsables de traitement et à leurs sous-traitants

Article 12

L'article 35 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au début du premier alinéa, est ajoutée la mention : « I. – » ;

2° Sont ajoutés deux alinéas ainsi rédigés :

« Le présent I est applicable aux traitements ne relevant ni du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ni du chapitre XIII de la présente loi.

« II. – Dans le champ d'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, le sous-traitant respecte les conditions prévues par ce règlement. »

CHAPITRE IV

Dispositions relatives à certaines catégories particulières de traitements

Article 13

L'article 9 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au premier alinéa, les mots : « infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que » sont remplacés par les mots : « condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne peuvent être effectués que sous le contrôle de l'autorité publique ou » ;

2° Le 1° est complété par les mots : « ainsi que les personnes morales de droit privé collaborant au service public de la justice et appartenant à des catégories dont la liste est fixée par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, dans la mesure strictement nécessaire à leur mission » ;

3° Le 3° est ainsi rédigé :

« 3° Les personnes physiques ou morales, aux fins de leur permettre de préparer et, le cas échéant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci et de faire exécuter la décision rendue, pour une durée strictement proportionnée à ces finalités. La communication à un tiers n'est alors possible que sous les mêmes conditions et dans la mesure strictement nécessaire à la poursuite de ces mêmes finalités ; »

4° Il est ajouté un 5° ainsi rédigé :

« 5° Les réutilisateurs des informations publiques figurant dans les jugements mentionnés à l'article L. 10 du code de justice administrative et les décisions mentionnées à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées. »

Article 14

I. – L'article 36 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au premier alinéa, les mots : « historiques, statistiques ou scientifiques » sont remplacés par les mots : « archivistiques dans l'intérêt public, à des

fins de recherche scientifique ou historique ou à des fins statistiques » ;

2° Les deuxième à dernier alinéas sont supprimés ;

3° Sont ajoutés deux alinéas ainsi rédigés :

« Lorsque les traitements de données à caractère personnel sont mis en œuvre par les services publics d'archives à des fins archivistiques dans l'intérêt public conformément à l'article L. 211-2 du code du patrimoine, les droits prévus aux articles 15, 16 et 18 à 21 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ne s'appliquent pas dans la mesure où ces droits rendent impossible ou entravent sérieusement la réalisation de ces finalités. Les conditions et garanties appropriées prévues à l'article 89 du même règlement sont déterminées par le code du patrimoine et les autres dispositions législatives et réglementaires applicables aux archives publiques. Elles sont également assurées par le respect des normes conformes à l'état de l'art en matière d'archivage électronique.

« Un décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, détermine dans quelles conditions et sous réserve de quelles garanties il peut être dérogé en tout ou partie aux droits prévus aux articles 15, 16, 18 et 21 du même règlement, en ce qui concerne les autres traitements mentionnés au premier alinéa du présent article. »

II. – Au 4° du IV de l'article L. 1461-1 du code de la santé publique, le mot : « deuxième » est remplacé par le mot : « premier ».

Article 15

À la fin de la seconde phrase de l'article L. 212-4-1 du code du patrimoine, les mots : « à fiscalité propre » sont supprimés.

Article 16

I. – Le chapitre IX de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« CHAPITRE IX

« Traitements de données à caractère personnel dans le domaine de la santé

« Section 1

« Dispositions générales

« *Art. 53*. – Outre aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, les traitements contenant des données concernant la santé des personnes sont soumis aux dispositions du présent chapitre, à l'exception des catégories de traitements suivantes :

« 1° Les traitements relevant des 1° à 6° du II de l'article 8 ;

« 2° Les traitements permettant d'effectuer des études à partir des données recueillies en application du 6° du même II lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ;

« 3° Les traitements mis en œuvre aux fins d'assurer le service des prestations ou le contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ainsi que la prise en charge des prestations par les organismes d'assurance maladie complémentaire ;

« 4° Les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ;

« 5° Les traitements effectués par les agences régionales de santé, par l'État et par la personne publique qu'il désigne en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article L. 6113-8.

« *Art. 54*. – I. – Les traitements relevant du présent chapitre ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent. La garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public.

« II. – Des référentiels et règlements types, au sens des *a* bis et *b* du 2° du I de l'article 11, s'appliquant aux traitements relevant du présent chapitre

sont établis par la Commission nationale de l'informatique et des libertés, en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés.

« Les traitements conformes à ces référentiels peuvent être mis en œuvre à la condition que leurs responsables adressent préalablement à la Commission nationale de l'informatique et des libertés une déclaration attestant de cette conformité.

« Ces référentiels peuvent également porter sur la description et les garanties de procédure permettant la mise à disposition en vue de leur traitement de jeux de données de santé présentant un faible risque d'impact sur la vie privée.

« III. – Les traitements mentionnés au I qui ne sont pas conformes à un référentiel mentionné au II ne peuvent être mis en œuvre qu'après autorisation de la Commission nationale de l'informatique et des libertés.

« IV. – La Commission nationale de l'informatique et des libertés peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques.

« V. – La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être prolongé une fois pour la même durée sur décision motivée de son président ou lorsque l'Institut national des données de santé est saisi en application du second alinéa de l'article 61.

« Lorsque la Commission nationale de l'informatique et des libertés ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée acceptée. Cette disposition n'est toutefois pas applicable si l'autorisation fait l'objet d'un avis préalable en application de la section 2 du présent chapitre et que l'avis ou les avis rendus ne sont pas expressément favorables.

« *Art. 55*. – Par dérogation à l'article 54, les traitements de données à caractère personnel dans le domaine de la santé mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés, ayant pour seule finalité de répondre, en cas de situation d'urgence, à une alerte sanitaire et d'en gérer les suites, au sens de la

section 1 du chapitre III du titre I^er^ du livre IV de la première partie du code de la santé publique, sont soumis aux seules dispositions de la section 3 du chapitre IV du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

« Les traitements mentionnés au premier alinéa du présent article qui utilisent le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques sont mis en œuvre dans les conditions prévues à l'article 22 de la présente loi.

« Les dérogations régies par le premier alinéa du présent article prennent fin un an après la création du traitement si ce dernier continue à être mis en œuvre au delà de ce délai.

« *Art. 56*. – Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre au responsable de traitement de données autorisé en application de l'article 54 les données à caractère personnel qu'ils détiennent.

« Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission nationale de l'informatique et des libertés peut adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre.

« Lorsque le résultat du traitement de données est rendu public, l'identification directe ou indirecte des personnes concernées doit être impossible.

« Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.

« *Art. 57*. – Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux mentionnés à l'article 53.

« Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement de données, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit.

« *Art. 58.* – Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont individuellement informées conformément aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

« Toutefois, ces informations peuvent ne pas être délivrées si la personne concernée a entendu faire usage du droit qui lui est reconnu par l'article L. 1111-2 du code de la santé publique d'être laissée dans l'ignorance d'un diagnostic ou d'un pronostic.

« *Art. 59.* – Sont destinataires de l'information et exercent les droits de la personne concernée par le traitement les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou la personne chargée d'une mission de représentation dans le cadre d'une tutelle, d'une habilitation familiale ou d'un mandat de protection future, pour les majeurs protégés dont l'état ne leur permet pas de prendre seuls une décision personnelle éclairée.

« Par dérogation au premier alinéa du présent article, pour les traitements de données à caractère personnel réalisés dans le cadre de recherches mentionnées aux 2° et 3° de l'article L. 1121-1 du code de la santé publique ou d'études ou d'évaluations dans le domaine de la santé, ayant une finalité d'intérêt public et incluant des personnes mineures, l'information peut être effectuée auprès d'un seul des titulaires de l'exercice de l'autorité parentale s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de la recherche, de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de l'autorité parentale, des droits mentionnés au premier alinéa.

« Pour ces traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès aux données le concernant recueillies au cours de la recherche, de l'étude ou de l'évaluation. Le mineur reçoit alors l'information et exerce seul ses droits.

« Pour ces mêmes traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale,

en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique, ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel du remboursement des prestations en nature de l'assurance maladie et maternité et de la couverture complémentaire mise en place par la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle. Il exerce alors seul ses droits.

« *Art. 60*. – Une information relative aux dispositions du présent chapitre doit notamment être assurée dans tout 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 mentionné au présent chapitre.

« Section 2

« Dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé

« *Art. 61*. – Les traitements automatisés de données à caractère personnel dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis à la section 1 du présent chapitre, sous réserve de la présente section.

« L'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique peut se saisir ou être saisi, dans des conditions définies par décret en Conseil d'État, par la Commission nationale de l'informatique et des libertés ou le ministre chargé de la santé sur le caractère d'intérêt public que présentent les traitements mentionnés au premier alinéa du présent article.

« *Art. 62*. – Au titre des référentiels mentionnés au II de l'article 54 de la présente loi, des méthodologies de référence sont homologuées et publiées par la Commission nationale de l'informatique et des libertés. Elles sont établies en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés.

« Lorsque le traitement est conforme à une méthodologie de référence, il peut être mis en œuvre, sans autorisation mentionnée à l'article 54 de la présente loi, à la condition que son responsable adresse préalablement à la Commission nationale de l'informatique et des libertés une déclaration attestant de cette conformité.

« *Art. 63*. – Dans le cas où la recherche nécessite l'examen des caractéristiques génétiques, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données. Le présent article n'est pas applicable aux recherches réalisées en application de l'article L. 1131-1-1 du code de la santé publique.

« *Art. 64*. – L'autorisation du traitement est accordée par la Commission nationale de l'informatique et des libertés dans les conditions définies à l'article 54, après avis :

« 1° Du comité compétent de protection des personnes mentionné à l'article L. 1123-6 du code de la santé publique, pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine mentionnées à l'article L. 1121-1 du même code ;

« 2° Du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine, au sens du 1° du présent article. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la composition de ce comité et définit ses règles de fonctionnement. Les membres du comité d'expertise sont soumis à l'article L. 1451-1 du code de la santé publique.

« Les dossiers présentés dans le cadre de la présente section, à l'exclusion des recherches impliquant la personne humaine, sont déposés auprès d'un secrétariat unique assuré par l'Institut national des données de santé, qui assure leur orientation vers les instances compétentes.

« *Art. 65*. – Dans le respect des missions et des pouvoirs de la Commission nationale de l'informatique et des libertés et aux fins de renforcer la bonne application des règles de sécurité et de protection des données, un comité d'audit du système national des données de santé est institué. Ce comité d'audit définit une stratégie d'audit puis une programmation, dont il informe la commission. Il fait réaliser des audits sur l'ensemble des systèmes réunissant, organisant ou mettant à disposition tout ou partie des données du système national des données de santé à des fins de recherche, d'étude ou d'évaluation ainsi que sur les systèmes composant le système national des données de santé.

« Le comité d'audit comprend des représentants des services des ministères chargés de la santé, de la sécurité sociale et de la solidarité, de la Caisse nationale d'assurance maladie, responsable du traitement du

système national des données de santé, des autres producteurs de données du système national des données de santé, de l'Institut national des données de santé, ainsi qu'une personne représentant les acteurs privés du domaine de la santé. Des personnalités qualifiées peuvent y être désignées. Le président de la Commission nationale de l'informatique et des libertés, ou son représentant, y assiste en tant qu'observateur.

« Les audits, dont le contenu est défini par le comité d'audit, sont réalisés par des prestataires sélectionnés selon des critères et modalités permettant de disposer de garanties attestant de leur compétence en matière d'audit de systèmes d'information et de leur indépendance à l'égard de l'entité auditée.

« Le prestataire retenu soumet au président du comité d'audit la liste des personnes en charge de chaque audit et les informations permettant de garantir leurs compétences et leur indépendance.

« Les missions d'audit s'exercent sur pièces et sur place. La procédure suivie inclut une phase contradictoire. La communication des données médicales individuelles ne peut se faire que sous l'autorité et en présence d'un médecin, s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé.

« Pour chaque mission diligentée, des échanges ont lieu, si nécessaire, entre les personnes en charge des audits, le président du comité d'audit, le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la santé publique et le président de la Commission nationale de l'informatique et des libertés.

« Si le comité d'audit a connaissance d'informations de nature à révéler des manquements graves en amont ou au cours d'un audit ou en cas d'opposition ou d'obstruction à l'audit, un signalement est adressé sans délai par le président du comité d'audit au président de la Commission nationale de l'informatique et des libertés.

« Chaque mission diligentée établit un rapport relevant notamment les anomalies constatées et les manquements aux règles applicables aux systèmes d'information audités.

« Si la mission constate, à l'issue de l'audit, de graves manquements, elle en informe sans délai le président du comité d'audit, qui informe sans

délai le président de la Commission nationale de l'informatique et des libertés et le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la santé publique.

« En cas d'urgence, le directeur général de la Caisse nationale d'assurance maladie peut suspendre temporairement l'accès au système national des données de santé avant le terme de l'audit s'il dispose d'éléments suffisamment préoccupants concernant des manquements graves aux règles précitées. Il doit en informer immédiatement le président du comité et le président de la commission. Le rétablissement de l'accès ne peut se faire qu'avec l'accord de ce dernier au regard des mesures correctives prises par l'entité auditée. Ces dispositions sont sans préjudice des prérogatives propres de la Commission nationale de l'informatique et des libertés.

« Le rapport définitif de chaque mission est transmis au comité d'audit, au président de la Commission nationale de l'informatique et des libertés et au responsable du traitement audité.

« Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, précise la composition du comité et définit ses règles de fonctionnement ainsi que les modalités de l'audit. »

II. – Le code de la santé publique est ainsi modifié :

1° Au 7° de l'article L. 1122-1, la référence : « 57 » est remplacée par la référence : « 58 » ;

2° Au treizième alinéa de l'article L. 1123-7, la référence : « au I de l'article 54 » est remplacée par la référence : « à l'article 61 » ;

3° Au second alinéa du IV de l'article L. 1124-1, la référence : « du II de l'article 54 » est remplacée par la référence : « de l'article 64 » ;

4° Au 6° de l'article L. 1461-7, la référence : « 56 » est remplacée par la référence : « 57 » ;

5° La seconde phrase du sixième alinéa de l'article L. 6113-7 est ainsi rédigée : « Les conditions de cette désignation et les modes d'organisation de la fonction d'information médicale, en particulier les conditions dans lesquelles des personnels placés sous l'autorité du praticien responsable ou des commissaires aux comptes intervenant au titre de la mission légale de certification des comptes mentionnée à l'article L. 6145-16 peuvent contribuer au traitement de données, sont fixés par décret. »

Article 17

La seconde phrase de l'article L. 312-9 du code de l'éducation est complétée par les mots : « , ainsi qu'aux règles applicables aux traitements de données à caractère personnel ».

Article 18

I. – L'article L. 4123-9-1 du code de la défense est ainsi rédigé :

« *Art. L. 4123-9-1*. – I. – Le responsable d'un traitement, automatisé ou non, ne peut traiter les données dans lesquelles figure la mention de la qualité de militaire des personnes concernées que si cette mention est strictement nécessaire à l'une des finalités du traitement.

« À l'exclusion des traitements mis en œuvre pour le compte de l'État, des collectivités territoriales et de leurs groupements ainsi que des associations à but non lucratif, les responsables des traitements informent le ministre compétent de la mise en œuvre de traitements comportant, dans le respect de l'obligation prévue au premier alinéa du présent I, la mention de la qualité de militaire.

« Les personnes accédant aux données à caractère personnel de militaires peuvent faire l'objet d'une enquête administrative aux seules fins d'identifier si elles constituent une menace pour la sécurité des militaires concernés. Le ministre compétent peut demander au responsable de traitement la communication de l'identité de ces personnes dans le seul but de procéder à cette enquête. Celle-ci peut comporter la consultation de traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, selon les règles propres à chacun d'eux.

« Dans l'hypothèse où le ministre compétent considère, sur le fondement de l'enquête administrative, que cette menace est caractérisée, il en informe sans délai le responsable du traitement qui est alors tenu de refuser à ces personnes l'accès aux données à caractère personnel de militaires y figurant.

« II. – Sans préjudice du 1 de l'article 33 du 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, en cas de divulgation ou d'accès non autorisé à des données des traitements mentionnés au I du présent article, le responsable

du traitement avertit sans délai le ministre compétent.

« III. – Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les conditions d'application du présent article.

« IV. – Est puni :

« 1° D'un an d'emprisonnement et de 100 000 € d'amende le manquement, y compris par négligence, à l'obligation prévue au deuxième alinéa du I du présent article ;

« 2° De trois ans d'emprisonnement et de 300 000 € d'amende le fait de permettre aux personnes mentionnées au dernier alinéa du I l'accès aux données comportant la mention de la qualité de militaire contenues dans un traitement mentionné au présent article ;

« 3° De trois ans d'emprisonnement et de 300 000 € d'amende le fait pour un responsable de traitement de ne pas procéder, y compris par négligence, à la notification mentionnée au II. »

II. – Les responsables des traitements de données à caractère personnel comportant la mention de la qualité de militaire disposent, lorsque cette mention n'est pas strictement nécessaire à l'une des finalités du traitement, d'un délai d'un an à compter de la publication de la présente loi pour procéder à sa suppression ou à son remplacement par celle de la qualité d'agent public.

III. – Le dernier alinéa de l'article 226-16 et le second alinéa de l'article 226-17-1 du code pénal sont supprimés.

IV. – Les III et IV de l'article 117 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale sont abrogés.

CHAPITRE V

Dispositions particulières relatives aux droits des personnes concernées

Article19

Au premier alinéa de l'article 7 de la loi n° 78-17 du 6 janvier 1978 précitée, après le mot : « concernée », sont insérés les mots : « , dans les

conditions mentionnées au 11) de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ».

Article 20

La section 1 du chapitre II de la loi n° 78-17 du 6 janvier 1978 précitée est complétée par un article 7-1 ainsi rédigé :

« *Art. 7-1*. – En application du 1 de l'article 8 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans.

« Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur.

« Le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne. »

Article 21

I. – L'article 10 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« *Art. 10*. – Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

« Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception :

« 1° Des cas mentionnés aux *a* et *c* du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets

protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande ;

« 2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre I^er^ du titre I^er^ du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 8 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard.

« Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre I^er^ du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel. »

II. – Le comité éthique et scientifique mentionné à l'article L. 612-3 du code de l'éducation remet chaque année, à l'issue de la procédure nationale de préinscription et avant le 1^er^ décembre, un rapport au Parlement portant sur le déroulement de cette procédure et sur les modalités d'examen des candidatures par les établissements d'enseignement supérieur. Le comité peut formuler à cette occasion toute proposition afin d'améliorer la transparence de cette procédure.

Article 22

Après l'article L. 121-4-1 du code de l'éducation, il est inséré un article L. 121-4-2 ainsi rédigé :

« *Art. L. 121-4-2.* – L'autorité responsable des traitements de données à caractère personnel mis en œuvre dans les établissements publics d'enseignement scolaire met à la disposition du public le registre comportant la liste de ces traitements, établi conformément aux dispositions du 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 comportant la liste de ces traitements. »

Article 23

Le III de l'article 32 de la loi n° 78-17 du 6 janvier 1978 précitée est complété par un alinéa ainsi rédigé :

« Lorsque les données à caractère personnel sont collectées auprès d'un mineur de moins de quinze ans, le responsable de traitement transmet au mineur les informations mentionnées au I du présent article dans un langage clair et facilement accessible. »

Article 24

L'article 40 de la loi n° 78-17 du 6 janvier 1978 précitée est complété par un III ainsi rédigé :

« III. – Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste des traitements et des catégories de traitements autorisés à déroger au droit à la communication d'une violation de données régi par l'article 34 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité lorsque la notification d'une divulgation ou d'un accès non autorisé à ces données est susceptible de représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique. La dérogation prévue au présent III n'est applicable qu'aux seuls traitements de données à caractère personnel nécessaires au respect d'une obligation légale qui requiert le traitement de ces données ou à l'exercice d'une mission d'intérêt public dont est investi le responsable de traitement. »

CHAPITRE VI

Voies de recours

Article 25

L'article 43 *ter* de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au II, après les mots : « aux dispositions », sont insérés les mots : « du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou » ;

2° Le même II est complété par les mots : « au vu des cas individuels présentés par le demandeur, qui en informe la Commission nationale de l'informatique et des libertés » ;

3° Le III est ainsi rédigé :

« III. – Cette action peut être exercée en vue soit de faire cesser le manquement mentionné au II, soit d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis, soit de ces deux fins.

« Toutefois, la responsabilité de la personne ayant causé le dommage ne peut être engagée que si le fait générateur du dommage est postérieur au 24 mai 2018. » ;

4° Le IV est complété par un alinéa ainsi rédigé :

« Lorsque l'action tend à la réparation des préjudices subis, elle s'exerce dans le cadre de la procédure individuelle de réparation définie au chapitre X du titre VII du livre VII du code de justice administrative et au chapitre I^{er} du titre V de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^{e} siècle. »

Article 26

La section 2 du chapitre V de la loi n° 78-17 du 6 janvier 1978 précitée est complétée par un article 43 *quater* ainsi rédigé :

« *Art. 43* quater. – Toute personne peut mandater une association ou une organisation mentionnée au IV de l'article 43 *ter* aux fins d'exercer en son nom les droits prévus aux articles 77 à 79 et 82 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable de traitement ou son sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du chapitre XIII de la présente loi. »

Article 27

I. – La section 2 du chapitre V de la loi n° 78-17 du 6 janvier 1978 précitée est complétée par un article 43 *quinquies* ainsi rédigé :

« *Art. 43* quinquies. – Dans le cas où, saisie d'une réclamation dirigée

contre un responsable de traitement ou son sous-traitant, la Commission nationale de l'informatique et des libertés estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne à l'égard du traitement de ses données à caractère personnel, ou de manière générale afin d'assurer la protection de ces droits et libertés dans le cadre de sa mission, elle peut demander au Conseil d'État d'ordonner la suspension d'un transfert de données, le cas échéant sous astreinte, et elle assortit alors ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ainsi que de tous les actes pris par la Commission européenne relativement aux garanties appropriées dans le cadre des transferts de données mentionnées à l'article 46 du même règlement. Lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par une juridiction dans l'exercice de sa fonction juridictionnelle, la Commission nationale de l'informatique et des libertés peut saisir dans les mêmes conditions le Conseil d'État aux fins d'ordonner la suspension du transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de 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 dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de cette décision d'adéquation. »

II. – L'article 226-22-1 du code pénal est ainsi modifié :

1° Les mots : « , hors les cas prévus par la loi, » sont supprimés ;

2° Les mots : « la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 » sont remplacés par les mots : « l'Union européenne ou à une organisation internationale en violation du chapitre V du 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, ou des articles 70-25 à 70-27 ».

Article 28

En application de l'article 7 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, lorsque le traitement repose sur le consentement de la personne concernée, le responsable de traitement doit être en mesure de démontrer que les contrats qu'il conclut portant sur des équipements ou services incluant le traitement de données à caractère personnel ne font pas obstacle au consentement de l'utilisateur final dans les conditions définies au 11 de l'article 4 du même règlement.

Peut en particulier faire obstacle à ce consentement le fait de restreindre sans motif légitime d'ordre technique ou de sécurité les possibilités de choix de l'utilisateur final, notamment lors de la configuration initiale du terminal, en matière de services de communication au public en ligne et aux applications accessibles sur un terminal, présentant des offres et des conditions d'utilisation de nature équivalente selon des niveaux différenciés de protection des données personnelles.

TITRE III

DISPOSITIONS PORTANT TRANSPOSITION DE 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

Article 29

I. – Le début du V de l'article 32 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé : « V. – Sans préjudice de l'application des dispositions du chapitre XIII, les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un

traitement mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense ou la sécurité publique, dans la... *(le reste sans changement).* »

II. – Le VI de l'article 32 de la loi n° 78-17 du 6 janvier 1978 précitée est abrogé.

III. – Au premier alinéa de l'article 41 de la loi n° 78-17 du 6 janvier 1978 précitée, après les mots : « sécurité publique », sont insérés les mots : « , sous réserve de l'application des dispositions du chapitre XIII ».

IV. – À l'article 42 de la loi n° 78-17 du 6 janvier 1978 précitée, les mots : « prévenir, rechercher ou constater des infractions, ou de » sont supprimés.

Article 30

Le chapitre XIII de la loi n° 78-17 du 6 janvier 1978 précitée devient le chapitre XIV et, après le chapitre XII, il est rétabli un chapitre XIII ainsi rédigé :

« CHAPITRE XIII

« Dispositions applicables aux traitements relevant de 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

« Section 1

« Dispositions générales

« *Art. 70-1*. – Le présent chapitre s'applique, le cas échéant par dérogation aux autres dispositions de la présente loi, aux traitements de données à caractère personnel mis en œuvre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, par toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommés autorité compétente.

« Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour l'une des finalités énoncées au premier alinéa, par une autorité compétente au sens du même premier alinéa et où sont respectées les dispositions des articles 70-3 et 70-4. Le traitement assure notamment la proportionnalité de la durée de conservation des données à caractère personnel, compte tenu de l'objet du fichier et de la nature ou de la gravité des infractions concernées.

« Pour l'application du présent chapitre, lorsque les notions utilisées ne sont pas définies au chapitre I^er^ de la présente loi, les définitions de l'article 4 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité sont applicables.

« *Art. 70-2*. – Le traitement de données mentionnées au I de l'article 8 est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée.

« *Art. 70-3*. – Si le traitement est mis en œuvre pour le compte de l'État pour au moins l'une des finalités énoncées au premier alinéa de l'article 70-1, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au I de l'article 26 et aux articles 28 à 31.

« Si le traitement porte sur des données mentionnées au I de l'article 8, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au II de l'article 26.

« *Art. 70-4*. – Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 8, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.

« Si le traitement est mis en œuvre pour le compte de l'État, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue à l'article 30.

« Dans les autres cas, le responsable de traitement ou son sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du traitement de données à caractère personnel :

« 1° Soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable de traitement ne prenait pas de mesures pour atténuer le risque ;

« 2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

« *Art. 70-5*. – Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées au premier alinéa de l'article 70-1 ne peuvent être traitées pour d'autres finalités, à moins qu'un tel traitement ne soit autorisé par des dispositions législatives ou réglementaires ou par le droit de l'Union européenne. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité 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 européenne.

« Lorsque les autorités compétentes sont chargées d'exécuter des missions autres que celles exécutées pour les finalités énoncées au premier alinéa de l'article 70-1, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, 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 européenne.

« Si le traitement est soumis à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter.

« L'autorité compétente qui transmet les données n'applique pas, en vertu du troisième alinéa du présent article, aux destinataires établis dans les autres États membres de l'Union européenne ou aux services, organes et organismes établis en vertu des chapitres 4 et 5 du titre V du traité sur le fonctionnement de l'Union européenne des conditions différentes de celles applicables aux transferts de données similaires à l'intérieur de l'État membre dont relève l'autorité compétente qui transmet les données.

« *Art. 70-6*. – Les traitements effectués pour l'une des finalités énoncées au premier alinéa de l'article 70-1 autre que celles pour lesquelles les données ont été collectées sont autorisés s'ils sont nécessaires et proportionnés

à cette finalité, sous réserve du respect des dispositions prévues au chapitre I[er] et au présent chapitre.

« Ces traitements peuvent comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, pour l'une des finalités énoncées au premier alinéa de l'article 70-1.

« *Art. 70-7*. – Les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sont mis en œuvre dans les conditions prévues à l'article 36.

« *Art. 70-8*. – Les données à caractère personnel fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.

« *Art. 70-9*. – Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

« Aucune autre décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée.

« Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel mentionnées au I de l'article 8 est interdit.

« *Art. 70-10*. – Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant que dans les conditions prévues aux 1, 2 et 10 de l'article 28 et à l'article 29 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et au présent article.

« Les sous-traitants doivent présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière que le traitement réponde aux exigences du présent chapitre et garantisse la protection des droits de la personne concernée.

« Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable de traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de

personnes concernées, les obligations et les droits du responsable de traitement ainsi que les mesures techniques et organisationnelles destinées à garantir la sécurité du traitement, et prévoit que le sous-traitant n'agit que sur instruction du responsable de traitement. Le contenu de ce contrat ou de cet acte juridique est précisé par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés.

« Section 2

« Obligations incombant aux autorités compétentes et aux responsables de traitement de données à caractère personnel

« *Art. 70-11*. – Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition. À cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition.

« Dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité et de la fiabilité des données à caractère personnel et de leur niveau de mise à jour.

« S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 70-20.

« *Art. 70-12*. – Le responsable de traitement établit, dans la mesure du possible et le cas échéant, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que :

« 1° Les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;

« 2° Les personnes reconnues coupables d'une infraction pénale ;

« 3° Les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;

« 4° Les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales ou des contacts ou des associés de l'une des personnes mentionnées aux 1° et 2°.

« *Art. 70-13*. – I. – Afin de démontrer que le traitement est effectué conformément au présent chapitre, le responsable de traitement et son sous-traitant mettent en œuvre les mesures prévues aux 1 et 2 des articles 24 et 25 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et celles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel mentionnées au I de l'article 8 de la présente loi.

« II. – En ce qui concerne le traitement automatisé, le responsable de traitement ou son sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à :

« 1° Empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement ;

« 2° Empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée ;

« 3° Empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées ;

« 4° Empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes qui n'y sont pas autorisées à l'aide d'installations de transmission de données ;

« 5° Garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation ;

« 6° Garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données ;

« 7° Garantir qu'il puisse être vérifié et constaté *a posteriori* quelles données à caractère personnel ont été introduites dans les systèmes de

traitement automatisé et à quel moment et par quelle personne elles y ont été introduites ;

« 8° Empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée ;

« 9° Garantir que les systèmes installés puissent être rétablis en cas d'interruption ;

« 10° Garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système.

« *Art. 70-14*. – Le responsable de traitement et son sous-traitant tiennent un registre des activités de traitement dans les conditions prévues aux 1 à 4 de l'article 30 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité. Ce registre contient aussi la description générale des mesures visant à garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel mentionnées au I de l'article 8 de la présente loi, l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées et, le cas échéant, le recours au profilage.

« *Art. 70-15*. – Le responsable de traitement ou son sous-traitant établit pour chaque traitement automatisé un journal des opérations de collecte, de modification, de consultation et de communication, y compris les transferts, l'interconnexion et l'effacement, portant sur de telles données.

« Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date et l'heure. Ils permettent également, dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et les destinataires de celles-ci.

« Ce journal est uniquement utilisé à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données et à des fins de procédures pénales.

« Ce journal est mis à la disposition de la Commission nationale de l'informatique et des libertés à sa demande.

« *Art. 70-16*. – Les articles 31, 33 et 34 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité sont applicables aux traitements de données à caractère personnel relevant du présent chapitre.

« Si la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable de traitement établi dans un autre État membre de l'Union européenne ou à celui-ci, le responsable de traitement établi en France notifie également la violation au responsable de traitement de l'autre État membre dans les meilleurs délais.

« La communication d'une violation de données à caractère personnel à la personne concernée peut être retardée, limitée ou ne pas être délivrée dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant compte des droits fondamentaux et des intérêts légitimes de la personne, pour éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires, pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, pour protéger la sécurité publique, pour protéger la sécurité nationale ou pour protéger les droits et libertés d'autrui.

« *Art. 70-17*. – Sauf pour les juridictions agissant dans l'exercice de leur fonction juridictionnelle, le responsable de traitement désigne un délégué à la protection des données.

« Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, en fonction de leur structure organisationnelle et de leur taille.

« Les dispositions des 5 et 7 de l'article 37, des 1 et 2 de l'article 38 et du 1 de l'article 39 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, en ce qu'elles concernent le responsable de traitement, sont applicables aux traitements de données à caractère personnel relevant du présent chapitre.

« Section 3

« Droits de la personne concernée par un traitement de données à caractère personnel

« *Art. 70-18*. – I. – Le responsable de traitement met à la disposition de la personne concernée les informations suivantes :

« 1° L'identité et les coordonnées du responsable de traitement et, le cas échéant, celles de son représentant ;

« 2° Le cas échéant, les coordonnées du délégué à la protection des données ;

« 3° Les finalités poursuivies par le traitement auquel les données sont destinées ;

« 4° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ;

« 5° L'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et l'existence du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée.

« II. – En plus des informations mentionnées au I, le responsable de traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits :

« 1° La base juridique du traitement ;

« 2° La durée de conservation des données à caractère personnel ou, à défaut lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

« 3° Le cas échéant, les catégories de destinataires des données à caractère personnel, y compris ceux établis dans les États n'appartenant pas à l'Union européenne ou au sein d'organisations internationales ;

« 4° Au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.

« *Art. 70-19*. – La personne concernée a le droit d'obtenir du responsable de traitement la confirmation que des données à caractère

personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, le droit d'accéder auxdites données ainsi qu'aux informations suivantes :

« 1° Les finalités du traitement ainsi que sa base juridique ;

« 2° Les catégories de données à caractère personnel concernées ;

« 3° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des États n'appartenant pas à l'Union européenne ou au sein d'organisations internationales ;

« 4° Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, à défaut lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

« 5° L'existence du droit de demander au responsable de traitement la rectification ou l'effacement des données à caractère personnel, et l'existence du droit de demander une limitation du traitement de ces données ;

« 6° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ;

« 7° La communication des données à caractère personnel en cours de traitement ainsi que toute information disponible quant à leur source.

« *Art. 70-20*. – I. – La personne concernée a le droit d'obtenir du responsable de traitement :

« 1° Que soient rectifiées dans les meilleurs délais des données à caractère personnel la concernant qui sont inexactes ;

« 2° Que soient complétées des données à caractère personnel la concernant incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ;

« 3° Que soient effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable de traitement.

« II. – Lorsque l'intéressé en fait la demande, le responsable de traitement doit justifier qu'il a procédé aux opérations exigées en application du I.

« III. – Au lieu de procéder à l'effacement, le responsable de traitement limite le traitement :

« 1° Soit lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée sans qu'il soit possible de déterminer si les données sont exactes ou non ;

« 2° Soit lorsque les données à caractère personnel doivent être conservées à des fins probatoires.

« Lorsque le traitement est limité en application du 1° du présent III, le responsable de traitement informe la personne concernée avant de mettre fin à la limitation du traitement.

« IV. – Le responsable de traitement informe la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ainsi que des motifs du refus.

« V. – Le responsable de traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente de laquelle ces données proviennent.

« VI. – Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I et III, le responsable de traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité.

« *Art. 70-21*. – I. – Les droits de la personne physique concernée peuvent faire l'objet de restrictions selon les modalités prévues au II du présent article dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant compte des droits fondamentaux et des intérêts légitimes de la personne pour :

« 1° Éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires ;

« 2° Éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;

« 3° Protéger la sécurité publique ;

« 4° Protéger la sécurité nationale ;

« 5° Protéger les droits et libertés d'autrui.

« Ces restrictions sont prévues par l'acte instaurant le traitement.

« II. – Lorsque les conditions prévues au I sont remplies, le responsable de traitement peut :

« 1° Retarder ou limiter la communication à la personne concernée des informations mentionnées au II de l'article 70-18 ou ne pas communiquer ces informations ;

« 2° Refuser ou limiter le droit d'accès de la personne concernée prévu à l'article 70-19 ;

« 3° Ne pas informer la personne du refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ni des motifs de cette décision, par dérogation au IV de l'article 70-20.

« III. – Dans les cas mentionnés au 2° du II du présent article, le responsable de traitement informe la personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable de traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision et met ces informations à la disposition de la Commission nationale de l'informatique et des libertés.

« IV. – En cas de restriction des droits de la personne concernée intervenue en application des II ou III, le responsable de traitement informe la personne concernée de la possibilité d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés. Hors le cas prévu au 1° du II, il l'informe également de la possibilité de former un recours juridictionnel.

« *Art. 70-22*. – En cas de restriction des droits de la personne concernée intervenue en application des II ou III de l'article 70-21, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés.

« Les deuxième et troisième alinéas de l'article 41 sont alors applicables.

« Lorsque la commission informe la personne concernée qu'il a été

procédé aux vérifications nécessaires, elle l'informe également de son droit de former un recours juridictionnel.

« *Art. 70-23*. – I. – Les informations mentionnées aux articles 70-18 à 70-20 sont fournies par le responsable de traitement à la personne concernée par tout moyen approprié, y compris par voie électronique et, de manière générale, sous la même forme que la demande.

« II. – Aucun paiement n'est exigé pour prendre les mesures et fournir ces mêmes informations, sauf en cas de demande manifestement infondée ou abusive.

« En cas de demande manifestement infondée ou abusive, le responsable de traitement peut également refuser de donner suite à la demande.

« En cas de contestation, la charge de la preuve du caractère manifestement infondé ou abusif des demandes incombe au responsable de traitement auquel elles sont adressées.

« *Art. 70-24*. – Les dispositions de la présente section ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données et les conditions de rectification ou d'effacement de ces données ne peuvent être régis que par les dispositions du code de procédure pénale.

« Section 4

« Transferts de données à caractère personnel vers des États n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des États n'appartenant pas à l'Union européenne

« *Art. 70-25*. – Le responsable de traitement de données à caractère personnel ne peut transférer des données ou autoriser le transfert de données déjà transmises vers un État n'appartenant pas à l'Union européenne que lorsque les conditions suivantes sont respectées :

« 1° Le transfert de ces données est nécessaire à l'une des finalités énoncées au premier alinéa de l'article 70-1 ;

« 2° Les données à caractère personnel sont transférées à un responsable établi dans cet État n'appartenant pas à l'Union européenne ou au sein

d’une organisation internationale qui est une autorité compétente chargée des fins relevant en France du premier alinéa de l’article 70-1 ;

« 3° Si les données à caractère personnel proviennent d’un autre État, l’État qui a transmis ces données a préalablement autorisé ce transfert conformément à son droit national.

« Toutefois, si l’autorisation préalable ne peut pas être obtenue en temps utile, ces données à caractère personnel peuvent être transmises à nouveau sans l’autorisation préalable de l’État qui a transmis ces données lorsque cette nouvelle transmission est nécessaire à la prévention d’une menace grave et immédiate pour la sécurité publique d’un autre État ou pour la sauvegarde des intérêts essentiels de la France. L’autorité dont provenaient ces données personnelles en est informée sans retard ;

« 4° La Commission européenne a adopté une décision d’adéquation en application de l’article 36 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 précitée ou, en l’absence d’une telle décision, un instrument juridiquement contraignant fournit des garanties appropriées en ce qui concerne la protection des données à caractère personnel ou, en l’absence d’une telle décision et d’un tel instrument, le responsable de traitement a évalué toutes les circonstances du transfert et estime qu’il existe de telles garanties appropriées.

« Les garanties appropriées fournies par un instrument juridique contraignant mentionnées au 4° peuvent résulter soit des garanties relatives à la protection des données mentionnées dans les conventions mises en œuvre avec cet État n’appartenant pas à l’Union européenne, soit de dispositions juridiquement contraignantes exigées à l’occasion de l’échange de données.

« Lorsque le responsable de traitement autre qu’une juridiction effectuant une activité de traitement dans le cadre de ses activités juridictionnelles transfère des données à caractère personnel sur le seul fondement de l’existence de garanties appropriées au regard de la protection des données à caractère personnel, il avise la Commission nationale de l’informatique et des libertés des catégories de transferts relevant de ce fondement.

« Dans ce cas, le responsable de traitement doit garder trace de la date et de l’heure du transfert, des informations sur l’autorité compétente destinataire, de la justification du transfert et des données à caractère personnel transférées. Ces informations sont mises à la disposition de la Commission nationale de l’informatique et des libertés à sa demande.

« Lorsque la Commission européenne a abrogé, modifié ou suspendu une décision d'adéquation adoptée en application de l'article 36 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 précitée, le responsable de traitement peut néanmoins transférer des données à caractère personnel ou autoriser le transfert de données déjà transmises vers un État n'appartenant pas à l'Union européenne si des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ou si ce responsable estime, après avoir évalué toutes les circonstances du transfert, qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.

« *Art. 70-26*. – Par dérogation à l'article 70-25, le responsable de traitement de données à caractère personnel ne peut, en l'absence de décision d'adéquation ou de garanties appropriées, transférer ces données ou autoriser le transfert de données déjà transmises vers un État n'appartenant pas à l'Union européenne que lorsque le transfert est nécessaire :

« 1° À la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;

« 2° À la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit français le prévoit ;

« 3° Pour prévenir une menace grave et immédiate pour la sécurité publique d'un autre État ;

« 4° Dans des cas particuliers, à l'une des finalités énoncées au premier alinéa de l'article 70-1 ;

« 5° Dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les mêmes fins.

« Dans les cas mentionnés aux 4° et 5° du présent article, le responsable de traitement de données à caractère personnel ne transfère pas ces données s'il estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert envisagé.

« Lorsqu'un transfert est effectué aux fins de la sauvegarde des intérêts légitimes de la personne concernée, le responsable de traitement garde trace de la date et de l'heure du transfert, des informations sur l'autorité compétente destinataire, de la justification du transfert et des données à caractère personnel transférées. Il met ces informations à la disposition de la Commission nationale de l'informatique et des libertés à sa demande.

« *Art. 70-27.* – Toute autorité publique compétente mentionnée au premier alinéa de l'article 70-1 peut, dans certains cas particuliers, transférer des données à caractère personnel directement à des destinataires établis dans un État n'appartenant pas à l'Union européenne lorsque les autres dispositions de la présente loi applicables aux traitements relevant du même article 70-1 sont respectées et que les conditions ci-après sont remplies :

« 1° Le transfert est nécessaire à l'exécution de la mission de l'autorité compétente qui transfère ces données pour l'une des finalités énoncées au premier alinéa dudit article 70-1 ;

« 2° L'autorité compétente qui transfère ces données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public rendant nécessaire le transfert dans le cas considéré ;

« 3° L'autorité compétente qui transfère ces données estime que le transfert à l'autorité compétente de l'autre État est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun ;

« 4° L'autorité compétente de l'autre État est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié ;

« 5° L'autorité compétente qui transfère ces données informe le destinataire de la finalité ou des finalités pour lesquelles les données à caractère personnel transmises doivent exclusivement faire l'objet d'un traitement par ce destinataire, à condition qu'un tel traitement soit nécessaire.

« L'autorité compétente qui transfère des données informe la Commission nationale de l'informatique et des libertés des transferts répondant aux conditions prévues au présent article.

« L'autorité compétente garde trace de la date et de l'heure de ce transfert, des informations sur le destinataire, de la justification du transfert et des données à caractère personnel transférées. »

TITRE IV

DISPOSITIONS VISANT À FACILITER L'APPLICATION DES RÈGLES RELATIVES À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL PAR LES COLLECTIVITÉS TERRITORIALES

Article 31

Sans préjudice du dernier alinéa de l'article L. 5111-1 du code général des collectivités territoriales, peuvent être conclues entre les collectivités territoriales et leurs groupements des conventions ayant pour objet la réalisation de prestations de service liées au traitement de données à caractère personnel.

Les collectivités territoriales et leurs groupements peuvent se doter d'un service unifié ayant pour objet d'assumer en commun les charges et obligations liées au traitement de données à caractère personnel.

Article 32

I. – Dans les conditions prévues à l'article 38 de la Constitution et dans le respect des dispositions prévues aux titres I^{er} à III de la présente loi et au présent titre, le Gouvernement est autorisé à prendre par voie d'ordonnance les mesures relevant du domaine de la loi nécessaires :

1° À la réécriture de l'ensemble de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin d'apporter les corrections formelles et les adaptations nécessaires à la simplification et à la cohérence ainsi qu'à la simplicité de la mise en œuvre par les personnes concernées des dispositions qui mettent le droit national en conformité avec 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 et transposent 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, telles que résultant de la présente loi ;

2° Pour mettre en cohérence avec ces changements l'ensemble de la législation applicable à la protection des données à caractère personnel, apporter les modifications qui seraient rendues nécessaires pour assurer le respect de la hiérarchie des normes et la cohérence rédactionnelle des textes, harmoniser l'état du droit, remédier aux éventuelles erreurs et omissions résultant de la présente loi et abroger les dispositions devenues sans objet ;

3° À l'adaptation et à l'extension à l'outre-mer des dispositions prévues aux 1° et 2° ainsi qu'à l'application à Saint-Barthélemy, à Saint-Pierre-et-Miquelon, en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans les Terres australes et antarctiques françaises de l'ensemble des dispositions de la loi n° 78-17 du 6 janvier 1978 précitée relevant de la compétence de l'État.

II. – Cette ordonnance est prise, après avis de la Commission nationale de l'informatique et des libertés, dans un délai de six mois à compter de la promulgation de la présente loi.

III. – Un projet de loi de ratification est déposé devant le Parlement dans un délai de six mois à compter de la publication de l'ordonnance.

Article 33

I. – Le livre II du code de la consommation, dans sa rédaction résultant de l'article 48 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, est ainsi modifié :

1° La sous-section 4 de la section 3 du chapitre IV du titre II est abrogée ;

2° Au premier alinéa de l'article L. 242-20, la référence : « L. 224-42-3, » est supprimée.

II. – Le II de l'article 48 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique est abrogé.

TITRE V

DISPOSITIONS DIVERSES ET FINALES

Article 34

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifiée :

1° Au second alinéa du II de l'article 13, après la référence : « 3° », est insérée la référence : « du I » ;

2° L'article 15 est ainsi modifié :

a) Le quatrième alinéa est supprimé ;

b) Aux cinquième et sixième alinéas, après la référence : « 2° », est insérée la référence : « du I » ;

c) Au septième alinéa, après la référence : « 4° », est insérée la référence : « du I » ;

d) Le dernier alinéa est supprimé ;

3° Les troisième et dernier alinéas de l'article 16 sont supprimés ;

4° Au second alinéa de l'article 17, après la référence : « 2° », est insérée la référence : « du I » ;

5° Au second alinéa de l'article 21, après la référence : « 2° », est insérée la référence : « du I » ;

6° Au premier alinéa de l'article 29, la référence : « 25, » est supprimée ;

7° Le I de l'article 30 est ainsi modifié :

a) Au premier alinéa, le mot : « déclarations, » est supprimé ;

b) Aux 2° et 6°, la référence : « 25, » est supprimée ;

8° Le I de l'article 31 est ainsi modifié :

a) Au premier alinéa, la référence : « 23 à » est remplacée par la référence : « 26 et » ;

b) À la fin du 1°, les mots : « ou la date de la déclaration de ce

traitement » sont supprimés ;

9° À la seconde phrase du second alinéa du II de l'article 39, les mots : « ou dans la déclaration » sont supprimés ;

10° À l'article 42, la référence : « 25, » est supprimée ;

11° L'article 67 est ainsi modifié :

a) Au premier alinéa, les références : « 22, les 1° et 3° du I de l'article 25, les articles » sont supprimées ;

b) Le quatrième alinéa est supprimé ;

c) La seconde phrase de l'avant-dernier alinéa est supprimée ;

12° L'article 70 est abrogé ;

13° La seconde phrase de l'article 71 est supprimée.

Article 35

I. – Pour les traitements ayant fait l'objet de formalités antérieurement au 25 mai 2018, la liste mentionnée à l'article 31 de la loi n° 78-17 du 6 janvier 1978 précitée, arrêtée à cette date, est mise à la disposition du public, dans un format ouvert et aisément réutilisable pour une durée de dix ans.

II. – Par dérogation au premier alinéa de l'article 22 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la mise en œuvre des traitements comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques qui ont été autorisés avant le 25 mai 2018 en application des articles 25 et 27 de la même loi, dans leur rédaction antérieure à la présente loi, ne sont pas soumis à l'obligation d'être mentionnés dans le décret prévu au premier alinéa de l'article 22 de la loi n° 78-17 du 6 janvier 1978 précitée, sauf modification de ces traitements et au plus tard jusqu'au 25 mai 2020. Ces traitements restent soumis à l'ensemble des autres obligations découlant de la même loi et du 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.

Article 36

I. – L'article 230-8 du code de procédure pénale est ainsi rédigé :

« *Art. 230-8*. – Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent, qui, d'office ou à la demande de la personne concernée, ordonne qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire, ou qu'elles fassent l'objet d'une mention. La rectification pour requalification judiciaire est de droit. Le procureur de la République se prononce dans un délai de deux mois sur les suites qu'il convient de donner aux demandes qui lui sont adressées. La personne concernée peut former cette demande sans délai à la suite d'une décision devenue définitive de relaxe, d'acquittement, de condamnation avec dispense de peine ou dispense de mention au casier judiciaire, de non-lieu ou de classement sans suite. Dans les autres cas, la personne ne peut former sa demande, à peine d'irrecevabilité, que lorsque ne figure plus aucune mention de nature pénale dans le bulletin n° 2 de son casier judiciaire. En cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées, sauf si le procureur de la République en prescrit le maintien, auquel cas elles font l'objet d'une mention. Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision de relaxe ou d'acquittement devenue définitive, il en avise la personne concernée. En cas de décision de non-lieu ou de classement sans suite, les données personnelles concernant les personnes mises en cause font l'objet d'une mention, sauf si le procureur de la République ordonne l'effacement des données personnelles. Lorsque les données personnelles relatives à la personne concernée font l'objet d'une mention, elles ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues aux articles L. 114-1 et L. 234-1 à L. 234-3 du code de la sécurité intérieure et à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Les décisions du procureur de la République prévues au présent alinéa ordonnant le maintien ou l'effacement des données personnelles ou ordonnant qu'elles fassent l'objet d'une mention sont prises pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de l'intéressé.

« Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour

lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la durée de conservation des données personnelles.

« Les décisions du procureur de la République sont susceptibles de recours devant le président de la chambre de l'instruction.

« Le procureur de la République dispose pour l'exercice de ses fonctions d'un accès direct aux traitements automatisés de données à caractère personnel mentionnés à l'article 230-6. »

II. – À la dernière phrase du deuxième alinéa de l'article 230-9 du code de procédure pénale, les mots : « d'un » sont remplacés par les mots : « de deux ».

III. – Le premier alinéa de l'article 804 du code de procédure pénale est ainsi rédigé :

« Le présent code est applicable, dans sa rédaction résultant de loi n° du relative à la protection des données personnelles, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, sous réserve des adaptations prévues au présent titre et aux seules exceptions : ».

Article 37

Les titres I^er^ à III et les articles 34 et 35 entrent en vigueur le 25 mai 2018.

Toutefois, l'article 70-15 de la loi n° 78-17 du 6 janvier 1978 précitée entre en vigueur à une date fixée par décret, et au plus tard :

1° Le 6 mai 2023 lorsqu'une telle obligation exigerait des efforts disproportionnés ;

2° Le 6 mai 2026 lorsque, à défaut d'un tel report, il en résulterait de graves difficultés pour le fonctionnement du système de traitement automatisé.

La liste des traitements concernés par ces reports et les dates auxquelles, pour ces traitements, l'entrée en vigueur de cette obligation est reportée sont déterminées par voie réglementaire.

La seconde phrase du 2° de l'article 10 de la loi n° 78-17 du 6 janvier 1978 précitée, dans sa rédaction résultant de l'article 21 de la présente loi, entre en vigueur le 1^er^ juillet 2020.

L’article 22 entre en vigueur à compter de la rentrée de l’année scolaire 2018-2019.

Délibéré en séance publique, à Paris, le 14 mai 2018.

Le Président,
Signé : FRANÇOIS DE RUGY

ISBN 978-2-11-144697-7

ISSN 1240 - 8468

Imprimé par l'Assemblée nationale