Commission nationale de l'informatique et des libertés

Délibération n° 2020-051 du 8 mai 2020 portant avis sur un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire

NOR : *CNIX2011646X*

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre des solidarités et de la santé d'une demande d'avis concernant un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire ;

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

Vu le code de la santé publique ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8 ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu l'arrêté du 23 mars 2020 modifié prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire ;

Vu la délibération n° 2020-044 du 20 avril 2020 de la CNIL portant avis sur un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire ;

Après avoir entendu Mme Valérie PEUGEOT, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

La commission est saisie dans des conditions d'extrême urgence d'un projet de décret fixant les modalités dans lesquelles les systèmes d'information prévus à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire peuvent être mis en œuvre.

Elle souligne que le présent avis porte sur un projet de décret pris en application d'un projet de loi encore en cours de discussion au Parlement. Les observations qu'elle formule ne valent donc que sous réserve de l'adoption de la loi, et à la condition que celle-ci autorise ce qui figure dans le projet de décret.

Selon le projet de loi, l'objectif des systèmes d'information envisagés est de permettre :

- l'identification des personnes infectées, par l'organisation des examens de biologie médicale de dépistage et la collecte de leurs résultats ;
- l'identification des personnes présentant un risque d'infection, par la collecte des informations relatives aux contacts des personnes infectées et, le cas échéant, par la réalisation d'enquêtes sanitaires, en présence notamment de cas groupés ;
- l'orientation des personnes infectées et des personnes susceptibles de l'être, en fonction de leur situation, vers des prescriptions médicales d'isolement prophylactiques, ainsi que le suivi médical et l'accompagnement de ces personnes pendant et après la fin de ces mesures ;
- la surveillance épidémiologique aux niveaux national et local, ainsi que la recherche sur le virus et les moyens de lutter contre sa propagation.

L'intervention du législateur pour la mise en œuvre des systèmes d'information envisagés se justifie par la nécessité d'apporter une dérogation aux dispositions relatives au secret médical garanti par le code de la santé publique. Le projet de loi en cours de discussion prévoit que ce décret « *précise notamment, pour chaque autorité ou organisme* (…), *les services ou personnels dont les interventions sont nécessaires aux finalités* (…) *et les catégories de données auxquelles ils ont accès, la durée de cet accès, ainsi que les organismes auxquels ils peuvent faire appel, pour leur compte et sous leur responsabilité, pour en assurer le traitement, dans la mesure où la finalité mentionnée au 2° du même II le justifie* ».

La commission relève que l'aménagement d'une nouvelle dérogation au principe du secret médical entraîne le partage de données d'une très grande sensibilité susceptibles de concerner l'ensemble de la population, caractérisant ainsi une situation inédite.

Pour répondre à ces finalités, le projet de décret crée deux traitements de données à caractère personnel : « Contact Covid », mis en œuvre par la Caisse nationale d'assurance maladie (CNAM) et dont l'objet principal est de permettre la conduite des enquêtes sanitaires, et « SI-DEP » (système d'information national de dépistage), mis en œuvre par le ministère de la santé (direction générale de la santé), qui centralisera les résultats des tests au SARS-CoV-2. La commission relève que ces systèmes d'information, d'une part, ne font pas l'objet aux termes du

décret d'une mise en relation automatisée et, d'autre part, ne sont pas liés directement au projet d'application de suivi de contacts « StopCovid » qui devrait, le cas échéant, faire l'objet d'un encadrement réglementaire spécifique.

Les traitements envisagés s'inscrivent dans la mise en œuvre d'une stratégie sanitaire globale dans le contexte de l'épidémie de covid-19. Les finalités poursuivies, notamment la mise en œuvre d'une politique de dépistage et d'enquêtes sanitaires sur tout le territoire, apparaissent déterminées, explicitées et légitimes, conformément à l'article 5 du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après RGPD).

La commission souligne que l'atteinte portée à la vie privée par ces traitements n'est admissible que si cette politique constitue la réponse appropriée pour ralentir la propagation de l'épidémie, notamment dans le contexte du déconfinement de la population programmé à partir du 11 mai 2020. Si elle relève que tel est le cas, en l'état des avis scientifiques sur lesquels s'appuie le Gouvernement, elle insiste, comme l'a déjà fait le Conseil d'Etat dans son avis sur le projet de loi prorogeant l'état d'urgence sanitaire, pour que la nécessité de ces traitements de données à caractère personnel soit périodiquement réévaluée au vu de l'évolution de l'épidémie et des connaissances scientifiques.

La commission rappelle que, quel que soit le contexte d'urgence, des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel doivent être apportées.

Ainsi, au-delà de son l'avis sur ce projet de décret, la commission se montrera attentive aux conditions de mise en œuvre de ces traitements, notamment en ce qui concerne les mesures de sécurité prévues. A ce titre, elle demande à être informée des conditions de leur déploiement par la CNAM et le ministère, notamment dans le cadre de la réalisation et de l'évaluation des analyses d'impact relatives à la protection des données (AIPD) qui devront, pour chacun des traitements, être réalisées en application de l'article 35 du RGPD. La commission demande à ce que celles-ci lui soient transmises dans leur version définitive ainsi que, le cas échéant, leurs mises à jour.

Ce projet de décret appelle les observations suivantes de la commission :

A titre liminaire, la commission relève que le Gouvernement n'a pas entendu faire obligation aux patients de révéler l'identité des personnes avec lesquelles ils ont été en contact, ni aux personnes qui seraient contactées dans le cadre d'une enquête sanitaire de répondre à l'enquêteur. En revanche, les laboratoires effectuant les tests auront pour obligation de saisir les données à caractère personnel des personnes dépistées dans le SI-DEP. Par ailleurs, à l'heure où elle statue, la commission observe qu'il n'est pas fait obligation aux médecins d'inscrire leurs patients dans l'application « Contact Covid ». En tout état de cause, le refus des médecins, des patients ou des personnes « contacts » de participer aux enquêtes sanitaires ne saurait entraîner de conséquences de quelque ordre que ce soit (administrative, financière, prise en charge, etc.). La commission en prend acte et appelle à ce que ces éléments soient clarifiés d'ici l'entrée en vigueur du dispositif.

Au vu du caractère temporaire des systèmes d'information créés par le projet de loi, la commission préconise que ceux-ci restent indépendants d'autres traitements pour que la fin de leur mise en œuvre soit effective dans les délais prévus.

Concernant le traitement « Contact Covid » :

Le chapitre Ier du projet de décret organise les conditions de mise en œuvre du traitement « Contact Covid ». Ce traitement est mis en œuvre par la Caisse nationale de l'assurance maladie, sur le fondement de l'exécution d'une mission d'intérêt public (article 6-1-*e* du RGPD).

Sur les finalités :

Selon le ministère, les finalités du traitement « Contact Covid », telles que prévues par l'article 1er du projet de décret, sont de :

- collecter des informations nécessaires à la détermination des personnes ayant été en contact avec les personnes diagnostiquées comme porteuses du SARS-CoV-2 ou présentant des symptômes avérés ;
- contacter ces personnes pour assurer leur suivi et permettre leur prise en charge ;
- réaliser des enquêtes sanitaires ;
- assurer l'information des autorités compétentes pour adapter les mesures en fonction des circonstances des contaminations (identification d'un foyer/*cluster*, mise en quarantaine, etc.) ;
- permettre la prise en charge des examens de biologie médicale de dépistage pour les « cas contacts » le nécessitant ;
- permettre la dispensation des masques en officine pour les cas contacts le nécessitant ;
- informer les organismes qui assurent l'accompagnement social de certaines des personnes contactées ;
- assurer le pilotage et le suivi statistique des actions ;
- permettre la réalisation d'études, recherches et évaluation sur ces actions.

La commission considère que les finalités et fonctionnalités prévues par le projet de décret s'inscrivent dans celles prévues à l'article 6 (II) du projet de loi prorogeant l'état d'urgence sanitaire en cours de discussion et sont conformes aux dispositions de l'article 5-1-*b* du RGPD.

Au vu de l'ampleur du traitement et de la sensibilité des données qui y seront traitées, la commission rappelle que ces finalités doivent s'entendre strictement et que tout usage des données qui ne s'inscrirait pas dans celles-ci serait sanctionné pénalement.

Sur les catégories de données collectées :

L'article 2 du projet de décret énumère la liste limitative des catégories de données à caractère personnel qui pourront être collectées ; ces dernières pourront concerner la personne testée positive (dit « patient 0 »), chaque personne considérée comme contact à risque et les professionnels de santé ou établissements concernés.

La commission relève la très grande sensibilité de ces données. Certaines sont des données médicales et d'autres relèvent de la vie privée des personnes (lien entre le « patient 0 » et les cas contact, déplacements récents effectués, présence ou passage en EPHAD, en établissement de santé ou dans un établissement pénitentiaire, profession, etc.).

La commission rappelle que les données doivent être pertinentes au regard des finalités du traitement et rappelle le principe de minimisation des données qui doit conduire à ne collecter que les données strictement nécessaires. Les listes de catégories de données doivent être exhaustives et ne pourront excéder celles prévues par la loi lorsqu'elle sera promulguée.

Elle estime que la collecte des données prévues dans le projet de décret est pertinente sous les réserves qui suivent.

Elle relève en premier lieu que certaines catégories de données font l'objet d'une description imprécise et appelle le ministère à les détailler : donnée de « rang de naissance », « données relatives au médecin à l'origine de l'inscription dans le traitement », données relatives à la profession qui comprennent « notamment » la qualité de professionnel de santé.

En particulier, la commission s'interroge sur la catégorie des « données relatives au lien avec le patient 0 » qui, ainsi désignée, apparaît particulièrement large, intrusive et non pertinente. Dans l'hypothèse où la qualification de ce lien serait indispensable, la commission souhaite que celle-ci s'exprime sous forme de catégories génériques prédéfinies, à choisir dans un menu déroulant. La commission invite le ministère à clarifier ce point.

Elle souligne en deuxième lieu que certaines données ne paraissent pertinentes que dans le cadre des enquêtes spécifiques liées au suivi de cas groupés réalisées par les ARS.

En troisième lieu, la commission observe que des données à caractère personnel concernant la santé seront collectées (résultat du test et existence de symptômes). Le traitement de ces données sensibles se fonde sur l'article 9-2-*g* du RGPD (motif d'intérêt public important) et, à ce titre, doit « *être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* ».

La commission estime que ces données, en particulier parce qu'elles seront rendues accessibles à un nombre important de personnes ne relevant pas de l'équipe de soins au sens de l'article L. 1110-4 du code de la santé publique, doivent faire l'objet d'une protection particulière.

Le projet de décret limite ainsi leur collecte aux seules données relatives au caractère positif du test ou, pour un patient hospitalisé, à l'existence de symptômes associés à un scanner. Aucune autre donnée de santé ne pourra dès lors être collectée dans le cadre de « Contact Covid », notamment depuis les autres bases de données mises en œuvre par l'assurance maladie.

En quatrième lieu, le projet de décret prévoit également la collecte du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR). La commission prend acte de ce que cette collecte est justifiée par des motifs d'identitovigilance ainsi que pour permettre l'organisation et la prise en charge financière sans ordonnance des examens de biologie médicale ainsi que la distribution de masques.

En cinquième lieu, la commission observe que seules peuvent être issues de traitements déjà mis en œuvre par la CNAM au titre de l'une de ses missions les coordonnées de contact des personnes figurant dans « Contact Covid », – ce qui exclut la réutilisation de toute autre donnée de santé.

En sixième lieu, la commission rappelle que la minimisation de la collecte des données nécessite, dans une logique de protection des données dès la conception (« *privacy by design* »), certaines mesures fonctionnelles dans le paramétrage du traitement. Elle appelle notamment à exclure les zones « commentaires » ou « zones blocs notes » susceptibles de contenir des données non pertinentes. Lorsqu'un choix multiple est nécessaire, il doit être proposé au moyen de menus déroulants proposant des informations et appréciations objectives.

Enfin, de façon plus générale, la commission souligne que des instructions claires et uniformes – reprenant les consignes des autorités sanitaires – devront être données à l'ensemble des intervenants quant à la définition d'un « cas contact », qui conduira au traitement des données à caractère personnel le concernant. La formation et la sensibilisation régulières des personnels qui seront amenés à intervenir seront donc essentielles.

Sur les personnes pouvant consulter, enregistrer ou être destinataires des données :

L'article 3 du projet de décret énumère les catégories de personnes qui peuvent accéder au système d'information ou être destinataires des données contenues dans l'application « Contact Covid ». La commission souligne que les catégories prévues devront *in fine* correspondre à celles autorisées par la loi.

S'agissant des personnes pouvant consulter et enregistrer des données :

Le décret énumère les personnes pouvant accéder aux systèmes d'information. L'encadrement des accès à des données de santé est essentiel au regard des exigences prévues par l'article 9-2-*g* du RGPD rappelées ci-dessus.

A ce titre, la commission estime que la mention présente à l'article 3 du projet de décret selon laquelle les personnes consultent ou enregistrent les données « *dans la limite de leurs besoins d'en connaître* » constitue une garantie essentielle. Cette garantie doit notamment se traduire par des précisions supplémentaires dans le décret, par des limitations d'accès paramétrées dans le système d'information et par ses règles d'usages.

En premier lieu, la commission appelle à ce que, dans toute la mesure du possible, le décret précise les finalités au titre desquelles chaque catégorie d'accédant accède au système d'information et les données correspondantes.

Elle relève que d'ores et déjà le projet de décret distingue notamment les personnes qui, du fait de leur fonction, sont autorisées à consulter et enregistrer, d'une part, l'ensemble des données (médecins, membres des équipes d'enquête sanitaire, agents des ARS, etc.) et, d'autre part, certaines données énumérées limitativement (professionnels des laboratoires de biologie médicale et pharmaciens). Ces accès différenciés doivent se traduire par des limitations d'accès.

En deuxième lieu, il appartiendra au responsable de traitement « Contact Covid » de paramétrer ces accès en écriture et en lecture selon les fonctions de chacun des organismes ou personnes autorisés par le décret. Cette matrice d'habilitation doit être un élément central de la sécurité du traitement. Le responsable de traitement doit ainsi définir des profils fonctionnels strictement limités aux besoins d'en connaître pour l'exercice des missions des personnels habilités. Par ailleurs, des mesures devront être mises en place dès que possible, pour que, dans la mesure du possible, les personnes habilitées ne puissent accéder aux différentes données relatives aux personnes concernées que lorsqu'elles en ont effectivement besoin, et notamment, pour certaines personnes habilitées, uniquement en présence des personnes concernées. Ces mesures peuvent par exemple consister en l'attribution des droits d'accès par un supérieur hiérarchique, ou bien par la remise d'une information qui lui est spécifique (code confidentiel, QR code, etc.) à la personne concernée qui devra être transmis à la personne habilitée afin qu'elle puisse déverrouiller l'accès aux données.

En troisième lieu, la commission relève que le projet de décret autorise de nombreux organismes à consulter et/ou enregistrer des données. Le ministère indique, au regard des finalités poursuivies et des contraintes opérationnelles rencontrées, qu'il n'entend pas paramétrer le dispositif de façon à limiter davantage les accès aux seuls besoins de chaque type d'utilisateur, par exemple en restreignant la consultation à un périmètre géographique ou à certains cas contacts pertinents au regard de la mission d'un enquêteur.

La commission attire dès lors l'attention des organismes concernés sur la nécessité pour eux de recourir à un ensemble de mesures protectrices complémentaires.

Parmi ces mesures figurent l'information et la sensibilisation des personnels aux règles d'usage du système d'information. Chaque organisme dont les agents (organismes d'assurance maladie, ARS, service de santé des armées, etc.) ou personnels (laboratoires privés de biologie médicale, pharmaciens, personnes placées sous l'autorité d'un médecin) seront autorisés à consulter ou enregistrer des données, devra avoir sensibilisé ceux-ci à leurs obligations : protection des données à caractère personnel, respect du secret professionnel et risques de sanctions pénales encourues en cas de détournement de finalité du traitement.

Il serait pertinent qu'un engagement formalisé de respecter ces principes soit obtenu préalablement à l'habilitation, qui devra comprendre une information claire et complète sur les dispositifs de traçage des accès mis en place, permettant un contrôle régulier de l'utilisation des données contenues dans le traitement.

Il est également nécessaire de définir une politique d'habilitation de leurs agents très stricte afin que seuls ceux qui ont en besoin d'en connaître accèdent à « Contact Covid ». Les habilitations délivrées doivent être limitées dans le temps et régulièrement revues, notamment pour intégrer les éventuels départs d'agents ou changements d'affectation.

Enfin, la commission attire l'attention du ministère sur les très fortes garanties devant entourer la possible délégation de missions d'enquêtes sanitaires à d'autres organisations, dans le cadre de l'urgence sanitaire, notamment à des utilisateurs en dehors de la sphère des acteurs formés à l'accès et au traitement de données de santé au vu des risques que ferait peser une telle délégation compte tenu des mesures d'authentification prévues.

S'agissant des personnes destinataires des données :

Le projet de décret énumère également les personnes qui pourront être destinataires de certaines données.

D'une part, le projet de décret autorise la transmission de certaines données, via les préfectures, aux organismes « qui assurent l'accompagnement social » des personnes.

La commission relève le manque de visibilité sur ce volet de l'action publique et le manque de précision de ce terme, qui est susceptible de recouvrir de nombreux organismes.

La commission estime qu'au vu de la sensibilité des transferts d'informations envisagés et du contexte sanitaire particulier conduisant une personne à solliciter un accompagnement, la liste des organismes auxquels de telles données pourraient être transmises doit être précisément définie. La commission prend acte de l'engagement du ministère de préciser dans le projet de décret les catégories de destinataires qui pourraient avoir accès aux données dans ce cadre. Ces organismes devront en tout état de cause présenter les garanties requises par le RGPD en matière de traitement des données.

Par ailleurs, la commission demande à ce que le rôle des préfectures consiste uniquement à la transmission vers les organismes *ad hoc*, sans création ni conservation d'un fichier supplémentaire.

Surtout, la commission comprend que seules les données des personnes l'ayant expressément souhaité peuvent être transmises.

En tout état de cause, il appartient à la Caisse nationale de l'assurance maladie, en sa qualité de responsable de traitement, de ne transmettre des données qu'à des organismes en mesure d'assurer la sécurité des données qui seraient transmises.

D'autre part, le projet de décret prévoit que des organismes compétents en matière de santé publique (Agence nationale de santé publique, ministère de la santé [DREES], Plateforme des données de santé [PDS], etc.) peuvent être destinataires de certaines données sous forme « pseudonymisée ». La commission attire l'attention du

Gouvernement sur le fait que cette transmission devra être conforme à la loi telle qu'elle sera promulguée. Elle relève en outre que la liste précise des données transmises à chaque organisme n'est pas détaillée dans le projet de décret et demande donc qu'il soit complété.

S'agissant de la transmission d'informations à la CNAM et à la PDS, la commission prend acte qu'elle interviendra dans le strict respect des dispositions de l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire. Dès lors, il conviendra de s'assurer que les finalités des traitements qui seraient mis en œuvre dans ce cadre s'inscriront tant dans les finalités prévues par le projet de décret que par celles prévues par l'arrêté. La commission rappelle en outre que les seules données qui pourront être transmises dans ce cadre sont celles listées dans l'arrêté.

Sur la durée de conservation :

Le projet de décret prévoit que les données sont conservées dans le traitement « Contact Covid » pendant une durée maximale d'un an à compter de la date de la publication de la loi prorogeant l'état d'urgence sanitaire.

Si la commission ne sous-estime pas l'intérêt, dans une logique notamment de politique sanitaire et dans un contexte évolutif de connaissances sur l'épidémie, de conserver les données ainsi collectées pour une période d'un an, elle estime que ce seul impératif ne doit pas guider la détermination de la durée de conservation des données. Elle souhaite qu'à l'issue de trois mois d'usage du dispositif « Contact Covid », la pertinence de cette durée fasse l'objet d'une évaluation.

La commission prend par ailleurs acte de l'engagement du ministère de mettre en place un mécanisme qui basculera en archivage intermédiaire dans un délai de trois mois après la clôture d'une enquête, les données ne présentant plus d'utilité dans le cadre d'une enquête sanitaire. Ces données ne seront plus accessibles en base active de l'outil « Contact Covid ».

S'agissant des données qui seraient susceptibles d'être transmises à la CNAM et à la PDS, la commission estime, au vu notamment des finalités et des durées de conservation prévues tant dans le projet de décret que dans l'arrêté du 23 mars 2020, que les données de « Contact Covid » n'auront vocation à intégrer le système national des données de santé (SNDS) ou un entrepôt pérenne au sein de la PDS, que dans l'hypothèse où le droit commun l'autoriserait. A défaut de modification du cadre juridique applicable à la PDS et au SNDS à l'issue la durée de conservation prévue par le projet de décret, l'ensemble des données collectées pendant cette période devra être détruit.

La commission précise par ailleurs que les traitements mis en œuvre à partir des données transmises à la CNAM et à la PDS ne pourront, en dehors de la réalisation de nouvelles formalités, être mis en œuvre au-delà de l'état d'urgence sanitaire déclaré à l'article 4 de la loi du 23 mars 2020, comme le prévoit l'arrêté du 23 mars 2020.

Sur les droits des personnes :

La base légale de l'intérêt public sur laquelle repose le traitement rend applicable l'ensemble des droits prévus par le RGPD au bénéfice des personnes, à l'exclusion du droit à la portabilité.

La commission relève que, au-delà du caractère volontaire de la participation aux enquêtes, le projet de décret exclut le droit d'opposition, qui doit s'analyser comme la faculté, prévue par l'article 23 du RGPD, de limiter les droits des personnes pour, notamment, des objectifs importants de santé publique. Seul un droit d'opposition des personnes quant à la transmission de leurs données à la PDS est prévu.

Au vu des explications qui lui ont été fournies, notamment sur le risque de fragiliser l'identification de cas contacts et des chaines de contamination, la commission ne remet pas globalement en cause ce choix. Cependant elle invite le Gouvernement à minimiser les cas d'exclusion du droit d'opposition. De plus, elle souligne que cela renforce la nécessité de mettre en œuvre un mécanisme d'archivage intermédiaire des données afin, notamment, que les « cas contact » qui souhaiteraient ne plus voir rendues accessibles leurs données aux enquêteurs soient rapidement retirés de la base active.

La commission relève qu'un droit d'opposition est également prévu au bénéfice des « patients 0 » pour la divulgation de leur identité aux personnes contact. Le ministère a précisé que cette disposition, contraire au principe du consentement à la révélation de l'identité prévue à l'article 2 (I-1°-l), serait supprimée. La commission en prend acte et invite ainsi le ministère à faire mention du droit au retrait du consentement.

La commission attire l'attention du responsable de traitement sur la parfaite information qui devra être donnée aux personnes concernées quant au traitement de leurs données à caractère personnel, tant en cas de collecte directe (« patient 0 ») qu'en cas de collecte indirecte (« cas contacts »). A ce titre, une information précise et adaptée devra être apportée aux personnes concernées, dans un contexte sanitaire particulier.

Concernant le droit d'accès des personnes, la commission rappelle que celui-ci devra couvrir également les données de traçabilité afin d'assurer aux personnes concernées un très haut niveau de transparence. Ainsi, les personnes devraient pouvoir accéder au détail des opérations effectuées sur leurs données, à l'exclusion des données qui pourraient permettre l'identification des personnes habilitées ayant réalisé lesdites opérations.

Enfin, la commission relève que le projet de décret ne prévoit pas la mise en œuvre de procédés de décision automatisée (utilisation de traitements algorithmiques tels que ceux dits d'« intelligence artificielle ») ou de profilage.

Sur les mesures de sécurité :

A titre liminaire, au vu de la nature et du volume des données traitées ainsi que des risques pour les personnes en cas d'atteinte à la sécurité des données, la commission estime incontournable qu'un socle minimal de mesures de

sécurité soit mis en place afin de garantir un niveau de sécurité à l'état de l'art du secteur de la santé. A cet égard, la commission rappelle que le respect de l'obligation de sécurité prévue à l'article 5-1-*f* et à l'article 32 du RGPD constitue une condition de licéité du traitement et souligne l'importance des mesures techniques et organisationnelles permettant d'assurer, notamment, la confidentialité des données, la traçabilité des actions et leur imputabilité. La commission considère donc que la mise en œuvre du traitement « Contact Covid » devra en particulier garantir la maîtrise de l'authentification des personnes et de la traçabilité des actions des utilisateurs.

A cet égard, la commission relève qu'une AIPD est en cours de réalisation par l'assurance maladie. Elle estime que l'ensemble des risques résiduels majeurs identifiés à ce jour devra être traité avant la mise en œuvre de l'application.

Concernant les modalités d'authentification des personnes, la commission relève que le dispositif prévu par le projet de décret autorise l'authentification par identifiant et mot de passe seuls, ce qui n'est pas conforme aux préconisations de la PGSSI-S et aux recommandations de la commission concernant l'accès à des données de santé. La commission estime préférable que l'ensemble des personnes habilitées à accéder aux données traitées utilise un mécanisme d'authentification forte comportant plusieurs facteurs d'authentification.

Si la mise en place d'une telle mesure devait être différée compte tenu de délais de mise en œuvre, la commission invite le ministère à s'assurer *a minima* que la politique de mot de passe prévue sera conforme à sa délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, ainsi qu'à réaliser une surveillance renforcée du traitement afin de détecter toute utilisation anormale dès l'ouverture du service.

Par ailleurs, en cas d'ouverture du traitement à des personnes d'autres entités, la commission relève que les risques de contournement des mesures d'authentification seraient amplifiés et qu'une telle ouverture ne pourrait se faire que dans des conditions d'authentification parfaitement à l'état de l'art.

Concernant la traçabilité des actions, la commission relève que le décret prévoit la mise en place de mesures de traçabilité afin de permettre d'imputer de façon fiable toute opération réalisée par les personnes habilitées, y compris les opérations de recherche de patients ou de cas contact. Ces mesures de traçabilité sont applicables aux personnes listées à l'article 3 du projet de décret. Compte tenu des limitations en matière de gestion des accès et des habilitations, la commission estime que les mesures de traçabilité constituent l'une des pierres angulaires de la sécurité des traitements autorisés par le projet de décret.

En conséquence, celui-ci devrait prévoir la mise en place d'un mécanisme de surveillance et de scellement des traces, par exemple via des systèmes de détection automatique des connexions anormales ainsi que par la mobilisation d'équipes opérationnelles dédiées à l'analyse de ces traces de connexion, afin de garantir que d'éventuelles opérations illégitimes soient non seulement tracées mais effectivement détectées. A ce titre, la commission prend acte de ce qu'une supervision centralisée par un centre de sécurité opérationnel avec une gestion des alertes de sécurité est prévue et considère que ce système de supervision devrait inclure les alertes concernant la traçabilité des accès.

Concernant le système d'information national de dépistage « SI-DEP » :

Sur les finalités :

L'article 7 du projet de décret précise que le système d'information SI-DEP a pour finalités :

- de centraliser les résultats d'examens de dépistage du SARS-CoV-2 afin de les mettre à disposition des organismes chargés de déterminer les personnes ayant été en contact avec des personnes infectées ;
- de réaliser des enquêtes sanitaires en présence de cas groupés pour rompre les chaînes de contamination ;
- d'orienter, de suivre et d'accompagner les personnes concernées ;
- de faciliter le suivi épidémiologique aux niveaux national et local et la recherche sur le virus, de même que les moyens de lutter contre sa propagation.

La commission considère que les finalités prévues par le projet de décret s'inscrivent dans celles prévues à l'article 6 (II) du projet de loi prorogeant l'état d'urgence sanitaire et qu'elles sont déterminées, explicites et légitimes, conformément à l'article 5-1-*b* du RGPD.

Au vu de l'ampleur du traitement et de la sensibilité des données qui y seront traitées, la commission rappelle que ces finalités doivent s'entendre strictement et que tout usage des données qui ne s'inscrirait pas dans celles-ci est sanctionné pénalement.

Sur la responsabilité de traitement et la sous-traitance :

La CNIL prend acte de ce que le responsable de traitement du SI-DEP est le ministère, l'AP-HP étant désignée comme sous-traitant.

La commission rappelle qu'une convention devra être conclue avant toute mise en œuvre du traitement conformément à l'article 28 du RGPD.

Sur les catégories de données :

L'article 8 du projet de décret prévoit la collecte de données concernant la santé et de données relatives à l'identification (notamment le NIR), aux coordonnées et à la situation de la personne testée, à l'identification et aux cordonnées des médecins, aux caractéristiques techniques du prélèvement et aux résultats des analyses biologiques, comprenant un QR-code. Des données sont également collectées s'agissant de la personne de confiance qui aura été désignée par la personne faisant l'objet d'un examen de dépistage.

La commission relève, parmi les données collectées s'agissant de la situation des personnes concernées, une information relative aux personnes résidant en « hébergement collectif ». Elle invite le ministère à clarifier cette notion, notamment si elle devait comprendre, par exemple, des lieux de privation de liberté, ou encore des foyers ou centres d'accueil.

Elle s'interroge par ailleurs sur ce que recouvrent les termes « autre information technique » relatifs aux caractéristiques du prélèvement et recommande que cette information soit précisée ou supprimée. En ce sens, elle prend acte de l'engagement du ministère de ne pas prévoir de recueil d'informations dans des zones de texte libre.

Concernant les informations relatives aux résultats des analyses biologiques, la commission relève que la transmission du compte rendu d'analyse est prévue. Dans la mesure où son contenu n'est pas précisé dans le projet de décret, elle appelle l'attention du ministère sur le fait que la transmission de ce document ne doit pas avoir pour conséquence de révéler des informations qui ne seraient pas nécessaires eu égard aux finalités du traitement.

S'agissant du QR-code, la commission relève que si celui-ci ne contient pas de données identifiantes en tant que telles, le traitement envisagé a bien pour objet d'attribuer de façon unitaire un QR-code aux personnes testées comme positives. En conséquence, une fois cette attribution réalisée, le QR-code ne peut donc être considéré comme anonyme. La commission demande donc au ministère de supprimer le terme « anonyme » du projet de décret sur ce point.

S'agissant enfin des données de la personne de confiance, la commission demande que le projet de décret précise les modalités du recueil de ces données, en précisant les cas dans lesquels leur collecte serait nécessaire.

Sur le traitement du NIR, la commission prend acte de ce que le projet de décret en prévoit la possibilité, s'agissant de personnes et de finalités non prévues par les dispositions du code de la santé publique ou les dispositions du décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire. La commission prend acte de ce que cette collecte est justifiée par des motifs d'identitovigilance.

Sous ces réserves, la commission considère que ces catégories de données sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, conformément aux dispositions de l'article 5-1-*c* du RGPD.

Sur les destinataires des données :

L'article 9 du projet de décret prévoit limitativement les personnes qui peuvent accéder ou être destinataires des données contenues dans l'application SI-DEP.

La commission relève que le projet de décret autorise de nombreux organismes à être destinataires des données, pseudonymisées ou non, contenues dans SI-DEP, pour certains usages déterminés.

En premier lieu, sans remettre en cause la légitimité de ces accès, elle attire l'attention des organismes concernés sur la nécessité pour eux de définir une politique d'habilitation de leurs agents très stricte afin que seuls ceux qui en ont besoin accèdent à SI-DEP. Les habilitations délivrées doivent être régulièrement revues, notamment pour intégrer les éventuels départs ou changement d'affectation des agents. Il appartiendra au ministère de la santé ou, sous ses instructions, à son sous-traitant, de paramétrer ces accès en écriture et en lecture selon les fonctions de chacun des organismes ou personnes autorisés par le décret. Cette matrice d'habilitation doit être un élément central de l'AIPD.

En deuxième lieu, plus spécifiquement, la commission relève notamment qu'il est prévu que les enquêteurs auront accès à l'ensemble des données mentionnées à l'article 8 du projet de décret.

Elle considère cependant que l'accès de l'ensemble de ces personnes à l'ensemble des données, pour certaines desquelles une dérogation au secret médical a dû être aménagée par le législateur, n'apparaît pas nécessaire.

En ce sens, à titre d'exemple, le numéro du prélèvement et le compte rendu d'analyse ne paraissent pas nécessaires à la réalisation des investigations sur les personnes ayant été en contact avec des personnes testées positives au SARS-CoV-2.

Elle attire donc l'attention du ministère sur la nécessité de justifier, pour chaque catégorie de données dont le traitement est envisagé, du besoin d'en connaître de chaque catégorie de destinataires.

La commission estime qu'en cas d'impossibilité de définir des conditions d'accès limitées, notamment pour des besoins opérationnels impératifs, des mesures extrêmement protectrices doivent être mises en place.

Chaque organisme dont les agents (organismes d'assurance maladie, ARS, service de santé des armées, etc.) ou personnels (laboratoires privés de biologie médicale, pharmaciens, personnes placées sous l'autorité d'un médecin) seront autorisés à consulter ou enregistrer des données, devra avoir sensibilisé ceux-ci à leurs obligations : protection des données à caractère personnel, respect du secret professionnel, risques de sanctions pénales encourues en cas de détournement du traitement. Il serait pertinent qu'un engagement formalisé de respecter ces principes soit obtenu préalablement à l'habilitation. A ce titre, une information claire et complète devra leur être apportée sur les dispositifs de traçage des accès mis en place, permettant un contrôle régulier de l'utilisation des données contenues dans le traitement.

En troisième lieu, s'agissant de l'accès aux données par les personnels habilités de l'Agence nationale de santé publique (ANSP), la commission relève qu'il est prévu pour deux finalités distinctes, nécessitant la transmission de données d'une granularité différente. Ainsi les personnels de l'ANSP accéderaient, sous réserve d'habilitation :

– à l'ensemble des données listées à l'article 8 du projet de décret nécessaires à la réalisation des investigations sur les personnes ayant été en contact avec des personnes testées positives au SARS-CoV-2, au suivi et à l'accompagnement des personnes et à la réalisation des enquêtes sanitaires, comprenant possiblement des données nominatives ;

– dans le cadre de ses missions de surveillance épidémiologique, à des données pseudonymisées.

La commission attire l'attention du ministère sur la nécessité de distinguer les habilitations.

En quatrième lieu, le projet de décret prévoit que des organismes compétents en matière de santé publique (Agence nationale de santé publique, ministère de la santé [DREES], PDS, etc.) peuvent être destinataires de certaines données sous forme « pseudonymisée ». La commission attire l'attention du Gouvernement sur le fait que cette transmission devra être conforme à la loi telle qu'elle sera promulguée.

Elle relève en outre que la liste précise des données transmises n'est pas détaillée dans le projet de décret, et demande donc qu'il soit complété afin de mentionner la liste précise des données susceptibles d'être transmises à chaque organisme dans ce cadre.

S'agissant de la transmission d'informations à la CNAM et à la PDS, la commission prend acte qu'elle interviendra dans le strict respect des dispositions de l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire. Dès lors, il conviendra de s'assurer que les finalités des traitements qui seraient mis en œuvre dans ce cadre s'inscriront tant dans les finalités prévues par le projet de décret que par celles prévues par l'arrêté. La commission rappelle en outre que les seules données qui pourront être transmises dans ce cadre sont celles listées dans l'arrêté.

Sur l'information et les droits des personnes concernées :

La commission attire l'attention du ministère sur la nécessité de prévoir des modalités permettant une diffusion auprès de l'ensemble des personnes concernées d'une information claire, transparente et pédagogique.

En ce sens, elle invite le ministère à prévoir :

– la mise à disposition des laboratoires d'analyses et des médecins d'un document d'information, contenant l'ensemble des mentions prévues par l'article 13 du règlement général sur la protection des données, qui pourrait être remis aux personnes qui ne disposeraient pas d'un accès à Internet ou qui souhaiteraient disposer d'un tel document ;
– sur l'ensemble des supports d'information, la mention d'une adresse postale, en plus d'une adresse électronique, afin de permettre aux personnes concernées de demander des informations sur le traitement et d'exercer les droits par cette voie également.

La commission relève que le projet de décret exclut le droit d'opposition, ce qui doit s'analyser comme la mise en œuvre de la faculté, prévue par l'article 23 du RGPD, de limiter en particulier les droits des personnes pour notamment des objectifs importants de santé publique. Seul est prévu un droit d'opposition des personnes quant à la transmission de leurs données à la CNAM et à la PDS pour des traitements qui seraient mis en œuvre à des fins de recherche.

Elle invite à en informer très clairement les personnes concernées. Elle invite par ailleurs le ministère à prévoir des modalités permettant à chaque personne concernée de faire exercice de son droit d'opposition à la transmission d'informations à la CNAM et à la PDS de santé dès la création de la fiche la concernant dans le SI-DEP, par exemple par l'ajout d'une case à cocher par le personnel du laboratoire d'analyses.

Sur la durée de conservation :

Le projet de décret prévoit que les données sont conservées dans le traitement SI-DEP pendant une durée maximale d'un an à compter de la date de la publication de la loi prorogeant l'état d'urgence sanitaire.

Si la commission ne sous-estime pas l'intérêt, dans une logique notamment de politique sanitaire et dans un contexte évolutif de connaissances sur l'épidémie, de conserver les données ainsi collectées pour une période d'un an, elle relève que cette durée est fixée de manière générale, sans distinction des catégories de données traitées, des personnes qu'elles concernent ou des finalités pour lesquelles elles sont traitées. Elle souhaite, à l'issue de trois mois d'usage du dispositif, que la pertinence de cette durée indifférenciée fasse l'objet d'une évaluation et que la possibilité de supprimer certaines catégories de données soit étudiée.

S'agissant des données qui seraient susceptibles d'être transmises à la CNAM et à la PDS, la commission estime, au vu notamment des finalités et des durées de conservation prévues tant dans le projet de décret que dans l'arrêté du 23 mars 2020, que les données de SI-DEP n'auront vocation à intégrer le système national des données de santé (SNDS) ou un entrepôt pérenne au sein de la PDS, que dans l'hypothèse où le droit commun l'autoriserait. A défaut de modification du cadre juridique applicable à la PDS et au SNDS à l'issue de la durée de conservation prévue par le projet de décret, l'ensemble des données collectées pendant cette période devra être détruit. La commission précise par ailleurs que les traitements mis en œuvre à partir des données transmises à la CNAM et à la PDS ne pourront, en dehors de la réalisation de nouvelles formalités, être mis en œuvre au-delà de l'état d'urgence sanitaire déclaré à l'article 4 de la loi du 23 mars 2020, comme le prévoit l'arrêté du 23 mars 2020.

Sur les mesures de sécurité :

A titre liminaire, la commission estime qu'au vu de la nature, du volume des données traitées et des risques pour les personnes en cas d'atteinte à la sécurité des données, il apparait incontournable qu'un socle minimal de mesures de sécurité soit mis en place afin de garantir un niveau de sécurité à l'état de l'art applicable aux données de santé. A cet égard, la commission rappelle que le respect de l'obligation de sécurité prévue à l'article 5-1-*f* et à l'article 32 du RGPD constitue une condition de licéité du traitement et souligne l'importance des mesures techniques et organisationnelles permettant d'assurer notamment la confidentialité des données, la traçabilité des actions et leur imputabilité. La commission considère donc que la mise en œuvre du traitement SI-DEP devra en particulier

garantir la maîtrise de l'échange et l'hébergement des données, de l'authentification des personnes et de la traçabilité des actions des utilisateurs.

La commission relève qu'une AIPD est en cours de réalisation par le ministère.

Concernant l'échange et l'hébergement des données, la commission prend acte de ce que les données transmises par les laboratoires de biologie médicale, les concentrateurs de données et les organismes externes feront l'objet de mesures de chiffrement à l'état de l'art, et que les bases de données ainsi que les sauvegardes du traitement seront chiffrées. Elle rappelle que des algorithmes cryptographiques à l'état de l'art doivent être utilisés et recommande que la mise en œuvre de cette mesure de sécurité fasse partie des priorités du ministère.

Concernant les modalités d'authentification des utilisateurs habilités à accéder aux traitements, la commission prend acte du recours à une authentification forte utilisant un mot de passe et un code à usage unique pour l'accès de certaines catégories de personnes habilitées, qu'elle estime souhaitable pour l'ensemble des personnes habilitées à accéder aux données. Elle relève également que les patients testés peuvent être avertis du résultat de leur analyse par SI-DEP. Elle prend note de ce que le ministère s'engage à ce que les modalités d'authentification des patients préalablement à l'accès à leurs résultats soient rendues conformes à la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.

Concernant la traçabilité des actions, la commission relève que le décret prévoit la mise en place de mesures de traçabilité afin de permettre d'imputer de façon fiable toute opération réalisée par les personnes habilitées, y compris les opérations de recherche de patients. Ces mesures de traçabilité sont applicables tant aux médecins ou professionnels mentionnés aux articles 8 et 9 du projet de décret qu'aux administrateurs techniques. Compte tenu de l'absence de mécanisme de limitation du périmètre des accès, la commission estime que les mesures de traçabilité constituent l'une des pierres angulaires de la sécurité des traitements autorisés par le projet de décret. En conséquence, ce dernier devrait prévoir la mise en place d'un mécanisme de surveillance des traces, par exemple via des systèmes de détection automatique des connexions anormales et des équipes opérationnelles dédiées à l'analyse de ces traces de connexion, afin de garantir que d'éventuelles opérations illégitimes soient non seulement tracées, mais effectivement détectées.

A ce titre, la commission prend acte de ce qu'une supervision globale avec une gestion d'alertes de sécurité est prévue, et considère que ce système de supervision devrait inclure les alertes concernant la traçabilité des accès.

La présidente,
M.-L. Denis