Numérique

Margo Bernelin, Jessica Eynard

Margo Bernelin et Jessica Eynard, « Numérique », *Cahiers Droit, Sciences & Technologies*, 12 | 2021, 203-228.

Référence électronique
Margo Bernelin et Jessica Eynard, « Numérique », *Cahiers Droit, Sciences & Technologies* [En ligne], 12 | 2021, mis en ligne le 07 mai 2021, consulté le 23 septembre 2021. URL : http://journals.openedition.org/cdst/3558 ; DOI : https://doi.org/10.4000/cdst.3558

1Accepter d'écrire une chronique en droit du numérique relève du défi tant sont nombreux les domaines aujourd'hui soumis à l'emprise des outils numériques. Qu'il s'agisse de la commande d'un ouvrage en ligne, du paiement des impôts, de nos échanges sociaux ou encore de la planification d'un rendez-vous médical, etc., le numérique est incontournable, voire omniprésent. Il se caractérise par des formes d'automatisation des tâches plus ou moins approfondies, permises par les avancées de l'intelligence artificielle, à l'image des véhicules autonomes. L'être humain lui-même est devenu un objet numérisable à travers la traduction de ses caractéristiques physiques et comportementales sous forme de « gabarits informatiques ». Finalement, tout ce qui peut être représenté ou véhiculé au moyen du numérique entre dans le giron du terme avec, en son épicentre, les outils informatiques. La discipline juridique n'échappe pas à cette propagation du numérique avec l'adoption de règles spécifiques dans tous les champs du droit, que l'on pense au droit procédural, au droit des transports, au droit pénal ou encore au droit de la santé.

2La présente chronique aura pour ambition de sonder cette thématique en mettant en exergue les effets des outils techniques sur le droit. Elle consistera en une revue de l'actualité juridique en la matière, sans prétendre à l'exhaustivité rendue quasiment impossible par l'extension continue de la production juridique dans ce domaine. Elle sera également l'occasion de développer à chaque numéro telle ou telle question choisie.

3Nous tenons à remercier les professeurs Céline Castets-Renard et Antoine Latreille qui tenaient jusqu'ici la présente chronique – alors intitulée « Société de l'information » – et qui nous ont passé le flambeau. Cette première chronique porte sur la période d'octobre 2020 à février 2021. Cette période a été marquée par une production pléthorique et d'une grande variété dans ce champ du droit, qui témoigne d'un intérêt grandissant pour l'encadrement des pratiques en lien avec le numérique à l'image du *Rapport sur la politique publique de la donnée, des algorithmes et des codes sources*remis le 23 décembre 2020 au Premier ministre[1]. Face à cette « déferlante » de textes, la chronique propose un panorama (I), puis traite plus en profondeur trois thématiques : la mise en œuvre du virage numérique en santé (II), la réponse numérique à la crise sanitaire (Covid-19) (III), et enfin la politique de l'Union européenne en faveur du partage des données et de l'intelligence artificielle (IV).

J. E. et M. B.

I. Panorama

4**Drones.** L'utilisation par les autorités publiques de caméras aéroportées a fait l'objet d'une forte actualité en cette fin d'année 2020. Le Conseil d'État (CE) a rendu un avis sur ce thème le 20 septembre 2020 (n° 401 214)[2], ainsi qu'un arrêt en date du 22 décembre 2020[3]. Il en ressort que la captation d'images de personnes aux moyens de drones peut être qualifiée de « traitement de données personnelles ». Précisément, lorsque les images sont captées lors de manifestations, elles peuvent révéler l'appartenance politique, syndicale ou encore les convictions religieuses des individus, le respect de la loi Informatique et libertés ainsi que du RGPD (Règlement général de protection des données) s'imposant dès lors. Le CE précise qu'une loi devra intervenir pour fixer les finalités de l'emploi des caméras aéroportées et pour préciser les garanties apportées face aux risques d'atteinte aux libertés fondamentales. En l'absence de telles garanties, le CE a ordonné, le 20 décembre 2020, la suspension de l'utilisation de drones à des fins de vérification de l'application des mesures sanitaires à Paris. Parallèlement, et pour les mêmes motifs, la CNIL a rappelé à l'ordre le ministère de l'Intérieur sur l'utilisation de drones équipés de caméras pour vérifier l'application de ces mêmes mesures[4].

5**Reconnaissance faciale et authentification en ligne.** Le CE a rejeté, le 4 novembre 2020, la demande d'annulation du décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile » (Alicem)[5]. Alicem est une application qui permet, grâce à des outils de reconnaissance faciale, d'identifier le détenteur d'un passeport biométrique. Les demandeurs soutenaient que le consentement des utilisateurs de l'application n'était pas librement donné, l'internaute étant forcé d'utiliser l'application pour s'identifier et accéder à certaines démarches en ligne. Le CE rejette cet argument, indiquant que l'internaute peut refuser d'utiliser Alicem et préférer s'identifier par la plateforme *FranceConnect*. Ainsi, pour le CE, l'existence d'une alternative technique emporte, en l'espèce, un consentement librement donné.

6**Sécurité intérieure.** Trois décrets ont été publiés en décembre 2020 pour étendre le champ des données collectées au sein de trois fichiers dédiés au maintien de la sécurité intérieure (les fichiers « Prévention des atteintes à la sécurité publique »[6], « Gestion de l'information et prévention des atteintes à la sécurité publique »[7], « Enquêtes administratives liées à la sécurité publique »[8]). Ces décrets ont fait l'objet de recours visant à suspendre leur exécution, recours rejetés par le Conseil d'État[9]. Dans ces décisions, le CE estime que les décrets en cause « limitent la collecte et l'accès aux données concernées au strict nécessaire pour la prévention des atteintes à la sécurité publique ou à la sûreté de l'État, ne portent pas une atteinte disproportionnée à la liberté d'opinion, de conscience et de religion, ou à la liberté syndicale ».

7**Assistants vocaux.** La CNIL a publié le 7 septembre 2020 son livre blanc sur les assistants vocaux[10]. Ces dispositifs techniques sont embarqués dans de nombreux objets, qu'il s'agisse des smartphones, voitures et autres objets connectés. La CNIL propose un état des lieux des enjeux posés par ces dispositifs, ainsi que des conseils à l'attention des concepteurs et utilisateurs. En substance, elle insiste sur les besoins de sécurité de ces assistants et sur la nécessaire information à fournir à l'utilisateur.

8**Cookies et traceurs.** La CNIL a publié le 17 septembre 2020 des recommandations sur le recours aux cookies et autres traceurs[11], lesquels ont pour fonction la transcription d'informations dans le terminal de communication électronique de l'utilisateur. Le document porte notamment sur l'information et le consentement des internautes, et rappelle que toute action passive de ce dernier équivaut à un refus d'utilisation de ces traceurs.

9**Transparence et classement en ligne.** Sur le fondement du Règlement (UE) 2019/1150 du Parlement et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, la Commission a publié le 8 décembre 2020 ses lignes directrices concernant la transparence en matière de classement en ligne opéré notamment par les moteurs de recherche[12]. On retiendra, entre autres, que ce document invite les entreprises à offrir des explications pertinentes et adaptées à un utilisateur « moyen » sur les critères qui ont présidé aux classements des sites répertoriés.

10**Marchés numériques.** Le 15 décembre 2020, la Commission européenne a publié sa proposition de règlement relative aux marchés numériques. Le texte entend encadrer les plateformes qui permettent la mise en rapport d'un internaute avec une entreprise utilisatrice de la plateforme. Les plateformes visées sont, par exemple, celles qui offrent des services d'intermédiation, les moteurs de recherche, les réseaux sociaux, les plateformes de partage de vidéos[13]. La proposition de règlement entend encadrer les pratiques jugées comme déloyales, et interdit, par exemple, aux plateformes de « combiner » sans consentement des données à caractère personnel qu'elles auraient recueillies avec d'autres bases de données.

11**Services numériques.** La Commission européenne a également publié une proposition de règlement sur les services numériques, laquelle entend actualiser les règles précédemment en vigueur relatives aux responsabilités et obligations des prestataires de services numériques[14]. Cette proposition impose, entre autres, des obligations de transparence, de notification et d'information des internautes, et prévoit le partage de certaines informations entre les plateformes et les États. Certaines de ces obligations ne visent que les « très grandes plateformes en ligne »[15].

12**Cybersécurité.** Le 16 décembre 2020, la Commission européenne a publié différents textes établissant sa « stratégie européenne de cybersécurité ». La Commission propose de réformer les règles relatives à la sécurité des réseaux et des systèmes d'information par l'adoption d'une nouvelle directive[16]. Elle entend ainsi créer de nouvelles obligations à la charge des États membres et de certaines entités pour protéger les infrastructures dites critiques[17]. Cette stratégie se compose également d'un rapport sur la mise en place des recommandations de la Commission sur les réseaux 5G[18], dont il ressort le besoin de suivre une approche coordonnée au niveau de l'UE pour assurer la cybersécurité de ces réseaux.

13**CJUE et numérique.** La Cour de justice de l'Union européenne (CJUE) a rendu divers arrêts dans le champ du droit du numérique, présentés ici pêle-mêle :

- Dans une espèce du 11 novembre 2020, la CJUE a indiqué que la clause précochée par le responsable d'un traitement de données personnelles concernant le consentement à la collecte et la conservation d'un titre d'identité ne respecte pas le droit de l'Union[19].
- La Cour a précisé, dans des arrêts du 6 octobre 2020, que le droit de l'Union interdit une réglementation nationale qui imposerait aux fournisseurs de communications électroniques la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation. Toutefois, en cas de menaces graves pour la sécurité nationale, un État peut imposer de telles mesures si elles sont limitées dans le temps[20].
- Dans un arrêt du 15 septembre 2020, la CJUE offre pour la première fois une interprétation du Règlement reconnaissant le

principe de « neutralité d'internet »[21], et précise qu'un fournisseur d'accès à internet ne peut privilégier certains services ou certaines applications en faisant bénéficier ses utilisateurs de « tarifs nuls » tandis qu'en parallèle il bloque ou ralentit le trafic pour d'autres services ou applications[22].

- La Cour s'est également intéressée aux applications sur smartphone qui mettent en relation des utilisateurs de services de taxi avec des chauffeurs. Dans un arrêt du 3 décembre, la CJUE a qualifié cet outil de « service de la société de l'information » au regard du droit de l'Union. En conséquence, une réglementation nationale peut, sous conditions, imposer un système d'autorisations préalables pour la fourniture de tels services[23].
- Enfin, dans un arrêt du 1er octobre 2020, la CJUE a également qualifié de « service de la société de l'information » la vente de médicaments en ligne, ce qui emporte l'interdiction pour un État membre de restreindre la circulation de ce service sauf pour des motifs d'intérêt général[24]. La Cour précise qu'« un État membre de destination d'un service de vente en ligne de médicaments non soumis à prescription médicale ne peut interdire à des pharmacies établies dans d'autres États membres vendant ces médicaments de recourir au référencement payant dans des moteurs de recherche et des comparateurs de prix », mais il peut en limiter la publicité et les offres promotionnelles.

II. La mise en œuvre du virage numérique en santé

14Lancée par le Gouvernement en 2019, la feuille de route du numérique en santé[25] s'appuie sur la loi de santé 2019[26] et vise au déploiement à large échelle de services et d'outils numériques dans le domaine de la santé. Elle comprend cinq objectifs : renforcer la gouvernance du numérique en santé, intensifier la sécurité[27] et l'interopérabilité[28] dans ce domaine, accélérer le déploiement des services numériques, soutenir la création de plateformes numériques pour le recueil des données de santé ainsi que leur consultation et, enfin, appuyer le développement de solutions numériques en santé. Différents textes adoptés en fin d'année 2020 contribuent à la mise en place de cette feuille de route (A). Présenté comme une opportunité par les pouvoirs publics, « le virage numérique » espéré apparaît délicat à bien des égards comme en témoigne le contentieux en la matière (B).

A. Mise en place de la feuille de route du numérique en santé

15On s'attachera ici au millefeuille dont la valeur normative est variable mais dont toutes les couches participent au déploiement des outils numériques en santé, qu'il s'agisse de l'identifiant national de santé (1), du dossier médical partagé (2), des prescriptions électroniques (3), ou encore de la doctrine du numérique en santé publiée par l'Agence du numérique en santé (4).

1. L'identifiant national de santé

• Décret n° 2019-1036 du 8 octobre 2019 modifiant le décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au Répertoire national d'identification des personnes physiques comme identifiant national de santé et les articles R. 1111-8-1 à R. 1111-8-7 du Code de la santé publique.
• Arrêté du 24 décembre 2019 portant approbation du référentiel « Identifiant national de santé ».
• Article 90, Loi n° 2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique.

16Afin d'atteindre les objectifs fixés par la feuille de route du numérique en santé et le déploiement de services dans ce domaine, il convient de pouvoir identifier informatiquement les patients. Pour ce faire, un identifiant national de santé (INS) individuel doit être créé. Comme l'indique l'article L.1111- 8-1 du Code de la santé publique, il se compose du « numéro d'inscription au Répertoire national d'identification des personnes physiques », plus communément nommé NIR ou numéro INSEE, comprenant les 15 chiffres du numéro de sécurité sociale. La création de l'INS suppose d'associer au NIR des données d'état civil (nom, prénoms, date de naissance, lieu de naissance, sexe). Cet INS, dont les modalités techniques ont été validées en 2019, doit progressivement être mis en place à partir du 1er janvier 2021. La loi d'accélération et de simplification de l'action publique, adoptée le 7 décembre 2020, met en lumière l'intérêt de cet identifiant. Son article 90 énonce que les données de santé seront rattachées à ce numéro. Ainsi, l'INS participe non seulement à l'identitovigilance[29], mais aussi à la numérisation et au partage des données de santé, qu'il s'agisse des données de soin courant ou, comme le précise cette même loi, des données de santé au travail. Les données précisément identifiées pourront contribuer à la prise en charge d'un patient par son médecin traitant ou par un autre professionnel de santé amené à intervenir, le cas échéant en urgence. L'article 90 de la loi précitée rappelle que le partage des données rattachées à l'INS doit se faire dans le cadre du secret professionnel, mais aussi des « règles de sécurité et d'interopérabilité », ces trois impératifs étant mis sur le même plan, alors même que les deux premiers visent la protection des données et de la vie privée des intéressés, tandis que le dernier sert, lui, à assurer le partage informatique des données entre des systèmes informatiques différents.

2. Le dossier médical partagé

• Article 98, loi n° 2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique.

17Créé en 2004, le dossier médical partagé (DMP)[30] est le socle de la feuille de route nationale du numérique en santé puisqu'il a vocation à accueillir les données numérisées de soin, de prise en charge des patients ainsi que d'autres données personnelles utiles aux professionnels de santé (emploi exercé par la personne, habitudes sportives et alimentaires, etc.). Ce dossier doit contribuer à une meilleure prise en charge des patients, les données étant accessibles par tout professionnel de santé quel que soit le lieu ou l'horaire. Cela doit permettre de prendre en charge en urgence un patient en s'appuyant sur les données versées dans le DMP par son médecin traitant (pathologies, les traitements en cours, etc.). En ce sens, l'article L.1111-14 du Code de la santé publique indique qu'« afin de favoriser la prévention, la coordination, la qualité et la continuité des soins, chaque personne dispose […] d'un dossier médical partagé ». Malgré cette utilité potentielle, le DMP n'a pas rencontré un franc

succès, peu de patients ayant effectué les démarches pour l'ouvrir en consentant à sa création, laquelle emporte nécessairement le traitement de ses données de santé et leur partage entre personnels soignants. Depuis 2019 cette situation devenait difficilement tenable en raison de la création automatique, pour chaque assuré, d'un espace numérique de santé (ENS) centralisant dans un espace en ligne ses données de santé telles que les données de remboursement de soins, les données que l'assuré souhaite lui-même verser, mais aussi le DMP (article L.1111-13 CSP et s.). L'ENS, créé non sans critique de manière automatique, donc sans le consentement des intéressés, serait demeuré incomplet, voire ineffectif en l'absence de l'ouverture tout aussi automatique du DMP[31]. L'article 98 de la loi n° 2020-1525 d'accélération et de simplification de l'action publique du 7 décembre 2020 revient sur ces difficultés en prévoyant, comme pour l'ENS, l'ouverture automatique du DMP et son versement lui aussi automatique à l'ENS. Le nouvel article L.1111-13 CSP indique ainsi que « le dossier médical partagé mentionné à l'article L. 1111-14 est intégré à l'espace numérique de santé dont il constitue l'une des composantes », et précise que « l'ouverture automatique de l'espace numérique de santé […] emporte la création automatique du dossier médical partagé ». Dès lors, cette ouverture automatique de l'ENS et du DMP impose au patient réfractaire à la centralisation de ses données de santé de s'opposer à ces ouvertures automatiques (système dit d'*opt-out*) dès lors qu'il en aura été informé[32].

3. Les prescriptions électroniques

• Ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique.
• Rapport au Président de la République relatif à l'ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique.

18Le virage numérique ne serait pas complet sans en dématérialiser un aspect central : les prescriptions « de soins, de produits ou de prestations » effectuées par des professionnels de santé. Les ordonnances papier sont donc vouées à disparaître au bénéfice d'un format électronique, lequel sera aisément consigné dans l'espace numérique de santé des Français. Forte d'une expérimentation lancée en 2019, l'ordonnance du 18 novembre 2020 autorise ces e-prescriptions qui sont encadrées par les articles L. 4071-1 et suivants du CSP, et dont les modalités d'application seront précisées par un futur décret. Toutefois, l'ordonnance fait l'objet de critiques en raison de l'exclusion de son champ, sans raisons apparentes, des prescriptions effectuées et exécutées au sein des établissements de santé, mais aussi à cause du rôle central assigné à la Caisse nationale d'Assurance maladie pour assurer la conception et la mise en œuvre de ces e-prescriptions[33]. Par ailleurs, les données issues de ces ordonnances seront transmises à la base de données de l'Assurance maladie sur les remboursements (Système national d'information interrégimes de l'assurance maladie) et donc versées au Système national des données de santé pour être utilisées à des fins de recherche.

4. Doctrine technique du numérique en santé et référentiel éthique

• Agence du numérique en santé et le ministère des Solidarités et de la Santé, Doctrine technique du numérique en santé, janvier 2021.

19La mise en place de la feuille de route du numérique en santé conduit à s'arrêter également sur un texte d'une normativité moins contraignante : la *Doctrine technique du numérique en santé* publiée en janvier 2021 par l'Agence du numérique en santé (ANS)[34]. Cette agence, souvent méconnue des juristes, a pour objet de « créer les conditions du développement des systèmes d'information, des services ou outils numériques utilisés dans le cadre de la prise en charge sanitaire et du suivi social et médico-social des usagers du système de santé, pour la coordination des actions des professionnels y concourant, ainsi que pour la télésanté, la recherche, le dépistage et la prévention, la veille et l'alerte sanitaires »[35]. Pour mener à bien ces missions, l'ANS participe à la création et à la validation de référentiels dans le champ de la santé numérique et publie chaque année un document intitulé *doctrine*. Selon l'ANS, « le document a pour objectif de décrire le cadre technique et le cadre d'urbanisation dans lesquels devront s'inscrire les services numériques d'échange et de partage de données de santé, en cible (à horizon trois ans) et en trajectoire »[36]. En pratique, ce document sert de guide pour suivre les avancées de la feuille de route du numérique en santé, avec des focus par exemple sur l'INS ou encore l'ENS[37]. Il permet également de présenter les nouveaux référentiels techniques validés par l'ANS et utiles pour les développeurs de services numériques.

20Le document constituerait-il un simple prospectus administratif à destination des professionnels du domaine ? Pas exactement, car il comprend notamment un référentiel « éthique » pour le déploiement du numérique en santé. Il énonce qu'« appliqués à l'éthique du numérique en santé, ces piliers [de l'éthique : autonomie, bienfaisance, non-malfaisance, justice] doivent ainsi concerner l'éthique des données, des algorithmes, des systèmes, des pratiques et des décisions (cf. intelligence artificielle). Si le RGPD (Règlement général de protection des données) est nécessaire pour pouvoir garantir une conformité éthique en matière de données et d'algorithmes, il n'est pas suffisant pour couvrir toutes les dimensions de l'éthique du numérique en santé »[38]. L'Agence prévoit alors « d'élaborer un référentiel de labellisation ou de certification éthique des outils numériques, que ce soient des services à destination des professionnels de santé, ou des applis mobiles notamment à destination des citoyens (dans la perspective du référencement pour les plateformes "bouquet de services" et "espace numérique de santé") »[39]. Ainsi, dans le domaine du numérique en santé, les règles relatives aux données et aux algorithmes contenues dans le RGPD seront complétées par des normes prévues dans le cadre d'un label ou d'une certification que les développeurs de services pourront choisir de suivre, la norme technique se faisant le relais de la norme éthique et légale.

21La *doctrine* propose également que l'ANS soit le moteur d'une refonte du Code de déontologie médicale afin que ce dernier intègre les dimensions éthiques du numérique et devienne un « code de e-déontologie » médicale. Si le document précise que ce travail nécessite la création d'actions et d'indicateurs de performances, il est frappant de noter qu'il ne cite pas le Conseil national de l'Ordre des médecins, pourtant en principe seul en charge de toute modification du Code de déontologie médicale.

22Une prochaine *doctrine technique* est attendue pour fin 2021 et sera soumise aux commentaires du public, elle révèle les enjeux du virage numérique amorcé, car les avancées de la feuille de route du numérique en santé conduisent à rendre quasi impossible pour un patient d'échapper à la numérisation de ses données de santé. Surtout, le partage de ces dernières n'est pas sans risque pour la vie privée. En effet, avec l'identifiant national de santé, les e-prescriptions et le dossier médical partagé, c'est un maillage numérique serré qui se met en place, dont on ne peut que difficilement s'extraire. Pour l'heure, les dispositifs créés vont se heurter au manque d'équipement informatique dont disposent les professionnels de santé en ville ou à l'hôpital, mais afin de remédier à ce constat, le « Ségur de la santé » dédie deux

milliards d'euros au numérique en santé pour contribuer à la mise à niveau informatique des structures de soin[40]. Le véritable virage est donc bien amorcé.

B. Numérique en santé : un virage délicat

23Le virage programmé et, on le voit, fortement accompagné par les pouvoirs publics n'est pas sans dangers ni dérives. Dès lors, il fait l'objet d'un contentieux assez foisonnant tant au regard des thèmes traités que des instances saisies. On s'arrêtera ici sur les sanctions prononcées par la Commission nationale informatique et libertés (CNIL) à l'encontre de deux médecins pour manquements aux obligations prévues par le RGPD (1) et sur une décision du tribunal judiciaire de Paris concernant deux sites internet proposant des téléconsultations (2).

1. Sanctions pour manquements à l'obligation d'assurer la sécurité des données et à l'obligation d'en notifier la CNIL

• CNIL, délibération de la formation restreinte n° SAN-2020-014 du 7 décembre 2020 concernant Monsieur […]
• CNIL, délibération de la formation restreinte n° SAN-2020-015 du 7 décembre 2020 concernant Monsieur […]

24La question de la sécurité et de la protection des données personnelles est bien au cœur du déploiement des outils numériques en santé. Des référentiels sont proposés par l'Agence du numérique en santé (ANS), lesquels viennent compléter les obligations imposées à la fois par le Code de la santé publique et par le RGPD afin de sécuriser l'hébergement des données et leur accès. Le maître mot est d'éviter que des tiers non habilités puissent accéder à des données de santé. La CNIL se charge de contrôler le respect du droit relatif aux données personnelles et c'est précisément l'autorité indépendante qui a sanctionné en cette fin d'année deux médecins libéraux pour le non-respect de ces règles de sécurité. Dans ces deux espèces, des données d'imagerie médicale (IRM, radiographies, scanners) associées à des noms, dates de naissance et dates de consultations des patients s'étaient retrouvées librement consultables et téléchargeables sur internet (pendant 4 mois dans la première espèce, 5 ans dans la seconde). Dans les deux affaires, les médecins en cause avaient paramétré leurs logiciels ou leur boxe internet afin de pouvoir accéder à distance aux données de leurs patients. La formation restreinte de la CNIL relève que « le traitement en cause concerne des données médicales, qui constituent des catégories particulières de données à caractère personnel, au sens de l'article 9 du Règlement. La nature de ces informations appelait donc une vigilance toute particulière afin d'éviter une violation de données ». La CNIL note par ailleurs « que la protection du réseau informatique interne et le chiffrement des données à caractère personnel font partie des exigences élémentaires en matière de sécurité informatique, qui incombent à tout responsable de traitement ». Les médecins n'ayant pas respecté ces exigences, la CNIL considère dès lors qu'en tant que responsables du traitement des données, ils ont manqué à l'obligation d'assurer la sécurité des données traitées telle que prévue à l'article 32 du RGPD. Le manquement à cette obligation est d'autant plus caractérisé « que des données de santé sont concernées et que cette catégorie particulière de données à caractère personnel doit bénéficier de mesures de sécurité renforcées ». De plus, la CNIL retient le manquement de ces médecins à l'obligation de notifier la CNIL de la violation du RGPD. En conséquence, elle prononce une amende administrative de 3 000 euros dans un cas et de 6 000,00 euros dans l'autre[41].

25Sur son site internet, la CNIL précise « assurer la publicité de ces décisions pour alerter les professionnels de la santé sur leurs obligations et la nécessité de renforcer leur vigilance sur les mesures de sécurité apportées aux données personnelles qu'ils traitent »[42]. Le message est donc clair : la mauvaise connaissance des outils informatiques ou les défaillances d'un prestataire devant assurer la connexion au réseau internet ne sont pas des motifs suffisants pour justifier les manquements des médecins à leurs obligations, la protection du réseau interne et le chiffrement des données étant considérés comme des exigences « élémentaires » pour tout responsable de traitement quel qu'il soit.

2. Téléconsultations et dérives

• Tribunal judiciaire de Paris en date du 6 novembre 2020, n° RG 20/54799, « arretmaladie.fr et docteursecu.fr ».

26Les activités de téléconsultation ont fortement augmenté pendant le confinement[43] et certaines ont fait l'objet de critiques, comme l'illustre la décision rendue par le tribunal judiciaire (TJ) de Paris en date du 6 novembre 2020. Cette affaire opposait le Conseil national de l'Ordre des médecins (CNOM) et la Caisse nationale de l'Assurance maladie (CNAM) aux sites internet « arretmaladie.fr » et « docteursecu.fr ». Ces deux sites proposaient des téléconsultations médicales en ligne et avaient laissé entendre plus ou moins directement que ces téléconsultations seraient remboursées par la Sécurité sociale, et donneraient lieu à des arrêts maladie. L'internaute devait simplement répondre à un questionnaire médical pour l'un des sites, et à une très courte visioconférence pour l'autre, le premier site renvoyant vers le second pour les téléconsultations. Face à ces pratiques, les demandeurs à l'instance souhaitaient, entre autres, obtenir la fermeture des sites. Ils faisaient valoir que ces derniers méconnaissaient les règles déontologiques de la profession de médecin en faisant, notamment, primer la volonté commerciale sur le soin des patients par la délivrance d'arrêts maladie de convenance, ce qui est interdit. Ils avançaient également une remise en cause de l'indépendance des médecins lorsque ces derniers sont poussés, par ces pratiques commerciales, à rédiger ces mêmes arrêts maladie. Pour les demandeurs, ces pratiques commerciales devaient être qualifiées de trompeuses dès lors qu'elles conduisaient à présenter les arrêts maladie comme des droits et que la mise en relation avec des médecins se faisait sans mention du fait que ces derniers se trouvaient à l'étranger et n'avaient pas le droit d'exercer en France. Enfin, les demandeurs s'interrogeaient sur la protection accordée aux données personnelles de santé par ces sites internet en raison du fait que ces données étaient échangées par des applications de discussions instantanées telles que « Whatsapp ».

27La société à l'origine du site « arretmaladie.fr » réfuta ces critiques, regrettant que les demandeurs aient mal interprété les informations présentées sur son site alors que les services de téléconsultation proposés étaient licites. Par ailleurs, elle soutient que les outils numériques utilisés pour échanger les données avec les patients présentaient des garanties suffisantes de protection des données personnelles. Quant à l'entreprise à l'origine du site « docteursecu.fr », les arguments avancés étaient sensiblement les mêmes, bien qu'ils aient dénoncé de surcroît le fait que le site « arretmaladie.fr » ait créé des liens hypertextes entre les deux sites internet, créant ainsi de la confusion quant aux motivations derrière leur propre site.

28Le TJ de Paris fait droit aux demandeurs et indique que le système opaque de rémunération des médecins, « ajouté à la célérité de la consultation, à l'impératif de rentabilité, et au caractère erratique de la consultation […], contrevient aux principes de la liberté d'exercice et de l'indépendance professionnelle et morale des médecins ainsi qu'aux principes

déontologiques fondamentaux que sont la liberté de prescription du médecin et le paiement direct des honoraires par le malade ». Il juge également que les règles relatives à l'hébergement des données de santé ne sont en l'espèce pas respectées. Par conséquent, le TJ de Paris ordonne la fermeture de ces deux sites.

29La décision souligne ainsi les difficultés juridiques soulevées par la rencontre entre la téléconsultation et la création de services en ligne dédiés[44]. Elle témoigne de ce que le déploiement du numérique en santé renouvelle l'étude de questions classiques en droit de la santé : l'indépendance des médecins, les conditions d'exercice de la médecine, les liens complexes entre les soins et le système de remboursement de ces derniers, la protection de la vie privée. Sur cette dernière thématique, rappelons que le Conseil national pilote de l'éthique du numérique avait exprimé ses inquiétudes en juillet 2020[45]. De fait, la téléconsultation ayant démontré sa praticité pendant la crise sanitaire, la dynamique ne risque pas de s'inverser dans les années à venir.

III. Covid-19 et outils numériques

30La pandémie de Covid-19 actuelle aura été l'occasion de déployer un arsenal numérique dans la « guerre » contre le virus. Ainsi deux systèmes d'information[46] ont-ils été mis en place : « SI-DEP » dédié à la centralisation des données de dépistage du virus et « Contact Covid » pour l'identification et la prise en charge des malades et des cas contacts[47]. De plus, un catalogue de données de santé spécifique à la Covid-19 a été créé et sa gestion confiée à la Plateforme nationale des données de santé (Health Data Hub). Ce catalogue comprend aussi bien des données de soin, de pharmacie, de dépistage ou encore des données relatives aux urgences ou à la prise en charge des malades[48]. Ces données sont accessibles pour des recherches entreprises en lien avec l'épidémie et pour la durée de l'état d'urgence sanitaire. Qu'il s'agisse des systèmes d'information ou du catalogue dédié du Health Data Hub, ces différents outils sont marqués à la fois par le manque d'information offerte au public quant à leur constitution, ce qu'a pu regretter la CNIL[49], mais aussi par le faible nombre de droits reconnus aux personnes dont les données sont centralisées par ces dispositifs. La fin d'année 2020 n'aura pourtant pas échappé à cette dynamique, avec la création de nouveaux outils ou l'aménagement des dispositifs précédents (A) et la volonté de les pérenniser au-delà de l'état d'urgence sanitaire (B).

A. La création de nouveaux outils et l'aménagement des dispositifs précédents

31Afin de contribuer à la lutte contre l'épidémie, le Gouvernement a créé un nouveau système d'information dédié au suivi de la vaccination contre la Covid-19 (1), tandis que les autres dispositifs ont fait l'objet de débats et de réaménagements (2)

1. Le système d'information « Vaccin Covid »

• Décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la Covid-19.

32Afin de contribuer à la gestion de la crise sanitaire, le Gouvernement a créé un nouveau système d'information (SI), c'est-à-dire une base de données, dédiée à la vaccination contre le virus. Publié le 25 décembre 2020, le décret n° 2020-1690 institue le SI dénommé « Vaccin Covid » lequel vise à l'identification des personnes vaccinées, à leur information, au suivi des stocks de vaccins et à la prise en charge financière de la vaccination. Afin d'identifier les personnes vaccinées, le SI est constitué, assez logiquement, de leur noms, coordonnées, sexe, date et lieu de naissance, ainsi que du numéro NIR. Le SI comprend également les références des vaccins, les informations relatives aux points de vaccination, aux effets indésirables et aux contre-indications en relation avec la vaccination. Le consentement à la vaccination emporte, sans possibilité de refus, le traitement des données personnelles au sein de ce SI, les individus disposant alors seulement du droit d'accès, de rectification et de limitation au traitement. Les données comprises dans le SI pourront venir enrichir le catalogue dédié à la Covid-19 du Health Data Hub, dès lors qu'elles auront été pseudonymisées[50], les individus pouvant s'opposer à un tel versement de leurs données.

33La création du SI « Vaccin Covid » est semblable aux autres SI dédiés à la lutte contre la pandémie. En effet, qu'il s'agisse de l'exhaustivité des données collectées, de leur sensibilité, des personnes habilitées à y accéder, des droits des individus ou bien encore de leur versement au Health Data Hub, les mêmes règles, peu ou prou, s'imposent. En revanche, à la différence des autres SI, le décret insiste sur l'information personnelle à délivrer non seulement à la personne vaccinée, mais aussi à celle qui envisage de l'être. À l'inverse, dans le cadre du SI-DEP, la personne qui entend se faire dépister ne bénéficie pas de mesures d'information spécifiques sur le devenir des données collectées dans le cadre d'un test[51]. De plus, le SI « Vaccin Covid » se distingue des autres bases de données en ce qu'il témoigne d'une volonté de contrôle. En premier lieu, il s'agit du contrôle des motifs médicaux justifiant l'accès à la vaccination, le fichier consignant les données de santé qui justifient l'éligibilité au vaccin. En second lieu, il s'agit du contrôle même de la vaccination. Il est alors difficile de ne pas faire de liens entre ce fichier et le projet de loi, déposé le 21 décembre 2020 à l'Assemblée nationale, proposant d'instituer un régime pérenne de gestion des urgences sanitaires. Ce dernier, s'il est voté en l'état, autorise le Premier ministre à interdire l'accès à certains lieux ou modes de déplacement à ceux qui ne pourraient présenter la preuve de l'administration d'un vaccin. Le SI « Vaccin Covid » pourrait alors assurer, à n'en pas douter, la mise en œuvre de cette disposition[52].

2. Débats et aménagement des SI-DEP et « Contact Covid »

• Conseil scientifique Covid-19, avis « Un nouvel ensemble numérique pour lutter contre le SARS-Cov-2 », 20 octobre 2020.
• Comité de contrôle et de liaison Covid-19, avis « Pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie », 15 septembre 2020.
• Loi n° 2020-1379 du 14 novembre 2020 autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire.

34Le Conseil scientifique Covid-19 et le Comité de contrôle et de liaison Covid-19 (CCL-Covid) ont tous deux publié des avis soutenant le déploiement d'outils numériques à des fins de gestion mais aussi de lutte contre la propagation du virus de la Covid-19. Conseillant le Gouvernement, ces deux organes ont mis en avant les bénéfices d'un maillage numérique étroit pour limiter la propagation du virus. En ce sens, le Conseil scientifique propose de tirer toutes les potentialités de l'application TousAntiCovid, du SI-Dep (dépistage) et de la plateforme de conseils en ligne « Mes conseils Covid », en informant de manière plus

personnalisée encore les citoyens sur la circulation du virus et sur les bons comportements à adopter, notamment en rapport avec l'âge ou du fait de certaines pathologies. Si elle est retenue, une telle proposition conduirait à aménager le cadre juridique existant pour créer des liens entre les outils numériques, favoriser le partage d'informations et, pour l'application TousAntiCovid, autoriser la collecte de données de santé directement identifiables afin de personnaliser l'information délivrée. Publié il y a quelques mois maintenant, l'avis du Conseil scientifique n'a, pour l'heure, pas été suivi pleinement. Seule l'application TousAntiCovid a évolué pour offrir davantage d'informations aux utilisateurs, mais sans prendre le chemin d'une véritable personnalisation.

35De son côté, le CCL-Covid regrette la faible interopérabilité entre les différents systèmes d'information (SI). De plus, à la différence du Conseil scientifique, le Comité de contrôle et de liaison Covid-19 (CCL-Covid) souligne la dépendance des SI et du maillage numérique vis-à-vis des moyens humains, lesquels font encore hélas défaut. En effet, le SI « Contact Covid » n'est utile que s'il est rempli dès qu'un patient est déclaré positif et si des « cas contacts » sont effectivement appelés et pris en charge. Cet avis du CCL-Covid met en lumière le constat, souvent vite évacué, selon lequel le « tout numérique » n'est pas autonome et suppose des moyens humains en amont et en aval afin de constituer une réponse pertinente à la crise sanitaire. Le CCL-Covid regrette également que le maillage numérique ne soit pas adapté aux personnes éloignées à la fois du système de soin, mais aussi des outils informatiques. Il suggère ensuite de modifier le droit existant afin d'autoriser la conservation des données des SI au-delà de la fin de l'état d'urgence sanitaire, afin de mener des recherches rétrospectives sur les données collectées.

36Ne donnant pas suite à ces propositions, la loi du 14 novembre 2020 prorogeant l'état d'urgence sanitaire vient toutefois aménager les dispositifs que sont le SI-DEP et « Contact Covid ». L'article 6 de la loi élargit la liste des groupes et personnels pouvant accéder aux données et aux organismes assurant l'accompagnement social des personnes. Le Conseil constitutionnel valide cet élargissement, indiquant qu'il se limite à un accès à certaines données et qu'il est conditionné par le consentement des personnes intéressées[53]. La loi votée précise, par ailleurs, le caractère obligatoire de la transmission des informations utiles par les professionnels soignants aux différents SI, sans que cette obligation soit assortie de sanctions spécifiques.

B. La pérennisation de certains dispositifs de collecte de données au-delà de la crise sanitaire

37Cherchant à pérenniser le modèle actuel de déploiement du numérique à des fins de gestion de l'épidémie, deux projets sont en cours d'examen à l'heure où ces lignes sont écrites : un projet de loi d'une part (1), de décret d'autre part (2).

1. Projet de loi nº 3714 instituant un régime pérenne de gestion des urgences sanitaires

• Projet de loi n° 3714 instituant un régime pérenne de gestion des urgences sanitaires, enregistré à l'Assemblée nationale le 21 décembre 2020.

38Tandis que les avis du CCL-Covid témoignent de la nécessité d'évaluer les systèmes d'information créés pendant l'état d'urgence sanitaire, selon un certain nombre de critères au rang desquels la capacité à détecter et casser les chaînes de transmission du virus, la capacité à minimiser les décès et les complications graves[54], le Gouvernement semble d'ores et déjà satisfait de ces outils et propose de les retenir dans le futur. En effet, le projet de loi instituant un régime pérenne de gestion des urgences sanitaires prévoit que « lorsqu'une situation sanitaire exceptionnelle rend nécessaires l'identification et le suivi des personnes affectées ou contaminées ou susceptibles de l'être, le ministre chargé de la Santé, les agences sanitaires nationales, les agences régionales de santé et les organismes d'Assurance maladie peuvent […] mettre en œuvre des traitements de données à caractère personnel concernant la santé des personnes, le cas échéant sans leur consentement ». Le SI alors créé sera intitulé SI-VIC pour « suivi des victimes de situations sanitaires exceptionnelles ». Après avis de la CNIL, un décret en Conseil d'État viendra fixer les caractéristiques essentielles de ce traitement de données et notamment la nature des données faisant l'objet d'un recueil.

39Par ailleurs, le projet de loi entend laisser la possibilité au directeur/directrice général de l'Union nationale des caisses d'Assurance maladie de « fixer les modalités de rémunération des professionnels de santé conventionnés participant à la collecte des données nécessaires au fonctionnement des traitements de données ». Le texte, proposé avec l'aval du Conseil d'État qui le juge proportionné aux objectifs poursuivis[55], autorise également le versement des données collectées au Système national des données de santé (SNDS), dont la gestion opérationnelle est assurée par le Health Data Hub. À la différence du système actuel, le SI créé ne constituera pas un catalogue particulier d'accès limité dans le temps. Par conséquent, toutes les données collectées seront conservées de manière pérenne à des fins de recherche, le cas échéant sans le consentement des individus en raison de l'urgence sanitaire de la situation. Pour évaluer ces systèmes d'information, le projet de loi suggère de conserver le Comité de contrôle et de liaison Covid-19 lequel sera aussi en charge « de vérifier tout au long de ces opérations le respect des garanties entourant le secret médical et la protection des données personnelles ». Il est regrettable que le texte n'indique pas comment ces prérogatives s'articuleront avec celles de la CNIL qui dispose de moyens et d'une expertise spécifique dans ce domaine.

2. Projet de décret sur le Health Data Hub

• Décret n° XXXX relatif au traitement de données à caractère personnel dénommé « Système national des données de santé ».
• Délibération n° XXXX du 29 octobre 2020 portant avis sur un projet de décret relatif au Système national des données de santé (demande d'avis n° 20011090).

40Le Système national des données de santé qui centralise les données de santé en France et dont la gestion opérationnelle est assurée par le Health Data Hub, est appelé à évoluer. Examiné en fin d'année 2020, un projet de décret revient sur la structuration des bases de données du SNDS (entre base principale et catalogues spécifiques), les rôles et obligations du HDH mais aussi de la Caisse nationale d'Assurance maladie, laquelle serait en charge du rassemblement des bases de données ainsi que de leur pseudonymisation. Le HDH serait, lui, responsable de l'enrichissement des bases de données. Le décret vient également préciser les données qui peuvent être versées au SNDS, et indique qu'il s'agit notamment des données

relatives aux conditions sociales, environnementales, aux habitudes de vie des personnes et au contexte socio-économique qui les caractérise. On se demande alors quelles données à caractère personnel pourraient encore échapper au SNDS. Et c'est l'avant-dernier article de ce décret qui indique que « les données, traitées sur le fondement de l'arrêté du 21 avril 2020 et appareillées au Système national des données de santé sont conservées dans le Système national des données de santé ». Les données collectées et remontées à la plateforme sont donc vouées non pas à être effacées de cette dernière au-delà de l'état d'urgence sanitaire, mais bien à s'y maintenir de manière pérenne. La CNIL, dans l'avis qu'elle a rendu à propos du décret, souligne que l'article en question ne permettra pas, malgré son intention, de conserver après la fin de l'état d'urgence sanitaire les données du catalogue Covid pour des recherches. En effet, le décret entend pérenniser la conservation des données qui auront été appareillées (c'est-à-dire couplées, associées) avec les bases de données du Système national des données de santé. La CNIL relève que le catalogue « Covid-19 » n'a précisément pas fait l'objet d'une telle association avec les autres bases de données du SNDS. La CNIL relève également que les données du SI-Dépistage et de « Contact Covid » ne doivent pas, aux termes de la loi du 7 août 2020, être conservées au-delà de six mois après la fin de l'état d'urgence sanitaire et, partant, un nouveau texte devrait intervenir pour autoriser une telle conservation au-delà de ce délai.

41Si ces projets de loi et de décret n'ont pas encore été adoptés, ils témoignent de la place centrale accordée aux outils numériques dans la gestion de la crise sanitaire en cours, mais aussi à venir, sans que cette place soit véritablement questionnée au-delà des avis du CCL-Covid.

IV. Union européenne : une politique en faveur du partage des données et de l'intelligence artificielle

42Dans son discours sur l'état de l'Union en septembre 2020, la présidente de la Commission européenne, Ursula von der Leyen, a rappelé la volonté d'impulser une dynamique « numérique » au sein de l'UE, les technologies numériques devant servir « à bâtir une société plus saine et plus verte »**56**. Il faudra chercher ailleurs toute critique du numérique, la présidente précisant vouloir faire « de la décennie qui s'ouvre la "décennie numérique" de l'Europe », avant de suggérer trois chantiers prioritaires à cet égard : les données, l'intelligence artificielle et les infrastructures de connectivité. Dans cette perspective, le dernier trimestre de l'année 2020 a été marqué par la publication de documents concernant deux thématiques, du reste poreuses : le partage des données au sein de l'Union européenne (A), d'une part, et l'intelligence artificielle, d'autre part (B).

A. Le partage des données au sein de l'Union

43Le partage des données est au cœur du projet européen, leur circulation devant participer au marché de l'Union. Pour favoriser ce partage, la Commission a publié sa proposition de

Règlement intitulée « Acte sur la gouvernance des données » (1), et envisage d'élargir les possibilités d'échange de données personnelles dans le domaine de la santé (2).

1. Gouvernance des données

• Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), 25 novembre 2020, COM/2020/767 final.

44Publiée le 25 novembre 2020, la proposition de règlement européen sur la gouvernance des données s'inscrit dans la volonté de soutenir et d'accélérer le partage des données au sein de l'Union européenne, et vient compléter la directive 2019/1024 sur les données ouvertes[57]. La définition de la donnée proposée par le texte est large et comprend « toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels » (article 2). Le texte organise la mise à disposition des données détenues par le secteur public, à l'exclusion de celles soumises aux droits d'autrui (à l'image des données à caractère personnel, des données soumises à des droits de propriété intellectuelle, ou encore des données couvertes par le secret des affaires). Sans surprise, la proposition exclut également de son champ les données des entreprises publiques, par des établissements d'enseignement ou encore lorsqu'elles sont protégées pour des raisons de sécurité nationale. Pour toutes les autres données, le texte organise alors les modalités de réutilisation sans pour autant créer de droit à la réutilisation au profit de tiers, les autorités publiques n'ayant pas l'obligation d'autoriser la réutilisation de leurs données (article 3(3)). À titre d'illustration, la proposition vient régir les cas dans lesquels des accords exclusifs de réutilisation des données, en principe interdits, peuvent, par dérogation, être conclus. La proposition indique que, si l'accord exclusif est nécessaire pour la fourniture d'un service ou d'un produit d'intérêt général, alors il peut être conclu. Cela sera notamment le cas lorsqu'une seule entreprise est en mesure technique d'analyser les données en question.

45Par ailleurs, la proposition entend institutionnaliser la mise à disposition volontaire de données visée par le règlement sous l'expression « d'altruisme en matière de données » et définie par l'article 2(10) du texte comme « le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou les autorisations accordées par d'autres titulaires de données pour l'utilisation de leurs données à caractère non personnel sans demander de contrepartie, à des fins d'intérêt général, telles que la recherche scientifique ou l'amélioration des services publics ». Cette institutionnalisation passe par la création d'un registre européen pour répertorier les organismes qui participent à cet « altruisme ».

46Enfin, consciente du fait que la réutilisation des données conduira à des politiques différentes selon les organismes publics des États membres, la Commission souhaite créer le « Comité européen de l'innovation dans le domaine des données », chargé de conseiller la Commission européenne sur la création de pratiques identiques et cohérentes, pour la gestion des demandes d'accès entre autres. Cette proposition de règlement, qui vient enrichir l'arsenal juridique européen concernant les données, devra s'articuler à la fois avec le RGPD[58] et avec la directive de 2019 sur les données ouvertes et la réutilisation des informations du secteur public[59]. Gageons que ce ne sera pas sans difficultés.

2. Espace européen des données de santé

• Consultation publique sur l'Espace européen des données de santé, 23 décembre 2020.
DG SANTÉ, Digital Health, European Reference Networks, A European Health Data Space, - Combined evaluation roadmap/ Inception impact assessment, 23 décembre 2020, Ares(2020)7907993 - 23/12/2020.

47La fin de l'année 2020 a également été propice à la création de catalogues de données au sein de l'Union européenne dans divers secteurs. Dans ce cadre, le programme dénommé Espace européen des données de santé (European Health Data Space) prend appui sur l'article 14 de la directive 2011/24/UE relative aux soins transfrontaliers[60], lequel prévoit la création d'un réseau entre les État membres volontaires pour le partage des données et le développement de services européens de santé en ligne. Les travaux de la Commission, publiés en fin d'année 2020, cherchent à dépasser le champ strict de la directive pour favoriser l'échange de données en dehors du cadre des soins transfrontaliers, par exemple pour la recherche scientifique. Pour ce faire, la Commission européenne a mis en ligne, le 23 décembre 2020, une consultation publique visant à faire le point sur les moyens de promouvoir l'échange de données de santé, les bénéfices attendus d'un tel partage au sein de l'UE au regard du développement de services numériques en santé, ainsi que sur les risques associés à l'IA en santé[61]. Cette consultation doit, entre autres, permettre d'analyser la nécessité d'adopter une nouvelle réglementation européenne en matière de libre circulation des services et produits numériques en santé. Il est regrettable que cette politique en faveur du partage et de la circulation de données aussi sensibles que les données de santé ne prenne pas suffisamment en compte les risques pour la vie privée des personnes concernées. Cette initiative s'inscrit toutefois dans une autre ambition : faire de l'IA un moteur économique pour l'UE.

B. Le déploiement de l'intelligence artificielle

48Depuis plusieurs années maintenant, l'intelligence artificielle est un thème d'intérêt pour l'UE et ses institutions[62], comme en témoignent les réflexions sur une possible reconnaissance d'une personnalité juridique pour les objets intelligents[63], sur l'encadrement des dispositifs de décision automatisée, ou encore sur les futurs droits des consommateurs[64]. La fin de l'année 2020 ne fait pas exception à cette dynamique, divers documents ayant été publiés par le Parlement en octobre (1), lesquels coïncident avec d'autres prises de position, européennes ou internationales (2).

1. Le Parlement européen et l'IA

• Parlement européen, rapport contenant des recommandations à la Commission concernant un cadre d'aspects éthiques en matière d'intelligence artificielle, de robotique et de technologies connexes (2020/2012(INL)).
• Parlement européen, résolution du 20 octobre 2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle (2020/2014(INL)).

• Parlement européen, résolution du 20 octobre 2020 sur les droits de propriété intellectuelle pour le développement des technologies liées à l'intelligence artificielle (2020/2015(INI)).

49Le Parlement européen a publié au mois d'octobre 2020 trois documents sur des thèmes complémentaires : l'éthique, la responsabilité civile et les droits de propriété intellectuelle. Le premier est un rapport adressé à la Commission européenne sur les aspects éthiques de l'IA, de la robotique et des technologies connexes. Le Parlement y livre une revue assez complète, il faut le reconnaître, des difficultés et questionnements les plus souvent évoqués lorsque l'on s'intéresse à l'IA. Il ne manque pas de mettre en avant les avancées permises par ces technologies**65**, mais il n'en ignore pas les inquiétudes qu'elles suscitent « concernant la capacité du cadre juridique actuel de l'Union, et notamment de l'acquis en matière de droit des consommateurs[…], de la législation relative à la protection des données, de la législation portant sur la sécurité des produits et la surveillance du marché, ainsi que de la législation anti-discrimination, à pouvoir encore effectivement faire face aux risques que posent l'intelligence artificielle, la robotique et les technologies connexes »**66**. En réponse à ce constat, le Parlement suggère de créer un cadre éthique robuste, notamment par l'intermédiaire d'un certificat européen de conformité éthique**67**, rejoignant ici les questionnements français sur l'intégration de référentiels éthiques de conformité en santé.

50Plus précisément, le Parlement propose une réglementation fondée sur une analyse des risques posés par l'IA, laquelle conduirait à adopter une réponse différenciée face à ces derniers. Dès lors, plus une technologie suscite de risques plus elle doit être encadrée pour garantir l'information des consommateurs, l'absence de biais et de discriminations, la liberté de pensée et d'expression, la protection de l'environnement, etc. Dans cette perspective, le Parlement suggère à la Commission de conduire des audits sur les incidences de l'IA dans certains champs et de retenir, le cas échéant, des règles sectorielles pour les transports, l'emploi, l'éducation, la santé, la sécurité intérieure, entre autres. Cette préférence pour une réglementation différenciée selon les risques encourus se retrouve dans la résolution adoptée le même jour par le Parlement au sujet de la responsabilité civile liée à l'IA. Au sein de ce deuxième texte, le Parlement précise que l'on peut qualifier les risques comme étant élevés lorsqu'il existe « une forte probabilité de porter préjudice à une ou plusieurs personnes, de manière aléatoire et au-delà de ce que l'on peut raisonnablement attendre ». Partant, c'est l'incertitude quant à la réalisation du risque qui se retrouve au cœur de cette définition, la notion d'aléa méritant, toutefois, davantage de précisions.

51En matière de responsabilité civile, le Parlement ne propose pas pour autant la rédaction d'un texte spécifique à l'IA, comprise comme des « systèmes de prise de décision automatisée », mais plutôt d'adapter la directive sur la responsabilité du fait des produits**68**, le cas échéant en la transformant en un règlement. Partant, le Parlement suggère judicieusement à la Commission de redéfinir les notions centrales de « produit », de « dommage », de « défaut » et de « producteur ». Selon le texte, cette dernière catégorie devrait comprendre « les fabricants, développeurs, programmeurs, prestataires de services et opérateurs ».

52Avec pertinence le Parlement s'attarde sur la notion d'opérateur dans toutes ses dimensions. Ainsi, l'opérateur est tout autant « la personne physique ou morale qui exerce un certain contrôle sur un risque associé à la mise en œuvre et au fonctionnement du système d'IA et tire profit de son exploitation », que celle « qui, de manière continue, définit les caractéristiques de la technologie, fournit des données ainsi qu'un service essentiel de soutien en amont, et exerce donc également un certain contrôle sur le risque lié à l'exploitation et au fonctionnement du système d'IA ». L'opérateur est jugé comme étant à l'origine des risques

encourus, et le consommateur doit, en conséquence, pouvoir engager sa responsabilité. En effet, c'est lui qui exerce un certain contrôle sur l'exploitation de l'IA « en déterminant les entrées, les sorties ou les résultats, ou pourrait modifier les fonctions ou processus spécifiques au sein dudit système ». Ces éléments définitionnels offriront, à n'en pas douter, un contentieux fourni si la proposition est adoptée, notamment pour ce qui concerne les notions de « contrôle » et de « continuité ».

53Si le Parlement entend encadrer l'IA, ses travaux démontrent une volonté parallèle d'encourager son développement par la reconnaissance de droits de propriété intellectuelle (PI) spécifiques. À l'inverse de la résolution sur la responsabilité civile, le Parlement suggère ici d'adopter un règlement spécifique à la question des droits de PI, reconnaissant un certain particularisme de l'IA en la matière. À titre d'illustration, le document indique que le droit actuel des brevets impose une description complète de l'invention, ce qui peut être ardu pour certaines technologies liées à l'IA tant les raisonnements embarqués sont complexes et difficilement accessibles. Par ailleurs, le document insiste sur la question de la protection des données, centrales au développement de l'IA, mais dont le cadre règlementaire doit encore être précisé notamment en ce qui concerne leur protection par le droit d'auteur.

2. Diverses prises de position sur l'IA

• FRA, Getting the future right – Artificial intelligence and fundamental rights, Vienne, 14 décembre 2020.
• Russell T. Vought, White House's memorandum on the regulation of AI applications, Washington DC, 17 novembre 2020, M-21-06.
• Conseil de l'Europe, Mise en place éventuelle d'un mécanisme de certification des outils et services d'intelligence artificielle dans le domaine juridique et judiciaire, étude de faisabilité réalisée par la Commission européenne pour l'efficacité de la justice, 8 décembre 2020, CEPEJ(2020)15 Rev.

54Les travaux du Parlement européen raisonnent à n'en pas douter avec ceux de l'Agence de l'Union européenne pour les droits fondamentaux, laquelle a publié en fin d'année 2020 un rapport intitulé « Bien préparer l'avenir : l'intelligence artificielle et les droits fondamentaux »[69]. Dans ce document, l'Agence interpelle les organes normatifs de l'Union en proposant que l'introduction de toute nouvelle politique dans le champ de l'IA prenne en compte les droits fondamentaux. Afin d'anticiper des difficultés sur ce registre, l'Agence suggère au législateur de l'Union de conduire des études d'impact et d'adapter le régime de responsabilité aux enjeux spécifiques posés par l'IA, rejoignant donc la position du Parlement.

55Les propositions du Parlement européen tranchent en revanche avec le parti pris outre-Atlantique de restreindre autant que possible l'encadrement de l'IA. Dans cette perspective, la note publiée par la Maison Blanche le 17 novembre 2020 à l'attention des directrices et directeurs d'agences fédérales à propos de l'IA conseille précisément d'éviter toute régulation contraignante en la matière. Le cas échéant, les agences doivent privilégier des approches ciblées en fonction des secteurs et des risques à la manière de ce qu'envisagent les textes européens[70].

56Enfin, ces annonces font écho à la publication, par le Conseil de l'Europe, d'une étude de faisabilité sur la « mise en place éventuelle d'un mécanisme de certification des outils et services d'intelligence artificielle dans le domaine juridique et judiciaire ». Le document

préconise la création d'un encadrement spécifique pour les technologies de fouille informatique de documents juridiques et la fourniture de services personnalisés pour répondre à des questions juridiques. Pour ce faire, le Conseil suggère lui aussi de recourir à la certification (de l'outil ou du service), laquelle devrait être « objective, neutre, visant l'application des droits de l'Homme dès la conception ». Le document précise alors que, « dans un secteur à haut risque, comme le secteur judiciaire, le caractère obligatoire d'une certification apparaît comme une caractéristique faisant consensus, mais dont la mise en œuvre ne doit pas brider l'innovation »[71]. Dès lors, le document détaille les critères pouvant constituer une base à la certification. Au rang de ces derniers on retrouve l'anonymisation des documents, le caractère explicable d'une décision rendue par l'IA ou encore la suppression de critères pouvant servir à des discriminations[72].

M. B.

Notes

1 É. Bothorel, S. Combes, R. Vedel, *Rapport sur la politique publique de la donnée, des algorithmes et des codes sources*, Paris, 23 déc. 2020.

2 CE, avis, 20 sept. 2020, n° 401 214, relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques.

3 CE, 22 déc. 2020, n° 446 155.

4 CNIL, délib. formation restreinte, *n° SAN-2021-003*, 12 janv. 2021, concernant le ministère de l'Intérieur.

5 CE, 4 nov. 2020, n° 432 656

6 D. n° 2020-1511, 2 déc. 2020, modifiant les dispositions du Code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Prévention des atteintes à la sécurité publique ».

7 D. n° 2020-1512, 2 déc. 2020, modifiant les dispositions du Code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Gestion de l'information et prévention des atteintes à la sécurité publique ».

8 D. n° 2020-1510, 2 déc. 2020, modifiant les dispositions du Code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique ».

9 CE, 4 janv. 2021, n^{os} 447868, 447869, 447870, 447879, 447881, 447882.

10 CNIL, *À votre écoute, Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux, 7 sept. 2020.*

11 CNIL, délib., *n° 2020-092*, 17 sept. 2020, portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ».

12 Commission européenne, Communication de la Commission Lignes directrices concernant la transparence en matière de classement, conformément au règlement (UE) 2019/1150 du Parlement européen et du Conseil, 8 déc., 2020/C 424/01.

13 Commission européenne, Proposition de Règlement relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), 15 déc. 2020, COM(2020) 842 final.

14 Commission européenne, Proposition de règlement relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, 15 déc. 2020, COM(2020) 825 final.

15 Il s'agit des « plateformes en ligne fournissant leurs services à un nombre mensuel moyen de bénéficiaires actifs du service au sein de l'Union égal ou supérieur à 45 millions » (article 25(1) de la Proposition.

16 Commission européenne, Proposed directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16 dec. 2020, COM(2020) 823 final.

17 Commission européenne, Proposed directive on the resilience of critical entities, 16 dec.2020, COM(2020) 829 final.

18 Commission européenne, Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks, 16 dec. 2020, SWD(2020) 357 final.

19 CJUE, 11 nov. 2020, C-61/19 (Orange România SA).

20 CJUE, arrêts dans l'affaire C-623/17 Privacy International et dans les affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., et C-520/18 Ordre des barreaux francophones et germanophone e.a., 6 oct. 2020.

21 Règl. (UE) n° 2015/2120 du Parlement européen et du Conseil, 25 nov. 2015, établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, et le Règl. (UE) n° 531/2012, concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union (Texte présentant de l'intérêt pour l'EEE)

22 CJUE, 15 sept. 2020, C-807/18 et C-39/19.

23 CJUE, 3 déc. 2020, C-62/19.

24 CJUE, 1er oct. 2020, C-649/18.

25 Ministère des Solidarités et de la Santé, *Feuille de route stratégique du numérique en santé* (Accélérer le virage numérique), Paris, 2019.

26 L. n° 2019-774, 24 juill. 2019, relative à l'organisation et à la transformation du système de santé.

27 La sécurité vise les moyens, le plus souvent techniques, utilisés pour empêcher des actions malveillantes sur des systèmes informatiques.

28 L'interopérabilité technique vise « l'interconnexion entre deux systèmes, s'appuyant sur l'utilisation d'interfaces définies, de normes et de protocoles partagés dans le respect des exigences de sécurité et de confidentialité des données personnelles de santé. » Agence du numérique en santé et le ministère des Solidarités et de la Santé, *Doctrine technique du numérique en santé*, janv. 2021, p. 32.

29 « L'identitovigilance est l'ensemble des mesures mises en œuvre pour fiabiliser l'identification de l'usager afin de sécuriser ses données de santé, à toutes les étapes de sa prise en charge. […] Les risques encourus en cas d'identification imparfaite sont nombreux. L'événement indésirable le plus fréquent est l'administration de soins au mauvais patient. L'identification erronée peut aussi être source : de retard de prise en charge, d'erreur diagnostique, d'erreur thérapeutique, d'échange d'informations erronées entre professionnels (imagerie, examens de biologie), d'enregistrement de données de santé dans le dossier d'un autre usager (collision), de création de plusieurs dossiers pour un même usager (doublons), d'erreur de facturation… », ministère de la Santé et des Solidarités, *Identitovigilance : Les bons soins au bon patient et au bon endroit*, 15 déc. 2020. Sur la question plus générale de l'identité numérique, v. J. Eynard (dir.), *Identité numérique, Quelle définition pour quelle protection ?*, Bruxelles, Larcier, 2020.

30 Créé par l'art. 3 de la loi n° 2004-810, 13 août 2004, relative à l'assurance maladie ; le dossier était dénommé à l'époque « Dossier médical personnel ».

31 À noter que l'ENS voté, n'est pas encore créé. Le 20 décembre dernier, le marché pour la création technique de l'ENS pour un montant 130 millions d'euros a été attribué, v. <https://www.boamp.fr/avis/detail/20-155197/officiel> dernier accès le 17 février 2021.

32 Un décret en Conseil d'État devra préciser les conditions de mise en œuvre du droit d'opposition, notamment l'information qui sera offerte à la personne.

33 Sur ces points, v. l'Union nationale des professionnels de la santé, avis du 15 juill. 2020 sur le projet d'ordonnance, <https://www.unps-sante.org/actualites/avis-de-l-unps-sur-le-projet-d-ordonnance-prescription-electronique/> dernier accès le 25 février 2021.

34 Agence créée en 2013 sous le nom « Agence nationale des systèmes d'information partagés de santé », v. la Convention constitutive de l'agence (GIP) du 23 mars 2013, <https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_conv-constit %20modifiee_25mars2013_signee.pdf> dernier accès le 12 janvier 2021.

35 Article 3.1 de la convention constitutive du groupement d'intérêt public « Agence nationale des systèmes d'information partagés de santé ».

36 Agence du numérique en santé et le ministère des Solidarités et de la Santé, *Doctrine technique du numérique en santé*, janvier 2021, p. 4.

37 Pour une illustration : p. 16 du document.

38 *Ibid.*, p. 26.

39 V. la p. 27 du document.

40 Ministère des Solidarités et de la Santé, *Ségur de la santé, les conclusions (dossier de presse*), juill. 2020, p. 20 (0,6 milliard sur cinq ans pour l'équipement des établissements médicaux-sociaux et 1,4 milliard sur trois ans pour rattraper « le retard sur le numérique en santé »).

41 L'amende est fonction du manquement constaté et des revenus des médecins.

42 <https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins> dernier accès le 15 février 2021.

43 <https://www.ticsante.com/story/5218/> dernier accès le 15 février 2021.

44 V. sur ce thème la chronique de L. Mazeau « Télémédecine et responsabilité civile des professionnels de santé », *CDST* 2020, n° 11, p. 227-234.

45 Conseil national pilote de l'éthique du numérique, *Enjeux d'éthique liés aux outils numériques en télémédecine et télésoin dans le contexte de la COVID-19*, Bulletin n° 3, 21 juill. 2020.

46 Un ensemble organisé de données diverses accessibles pour leur consultation.

47 D. n° 2020-551, 12 mai 2020, relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions.

48 Arr., 21 avr. 2020 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.

49 Commission nationale informatique et libertés (2020), d*élib. n° 2020-087*, 10 sept. 2020, portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de Covid-19 (mai à août 2020), Paris, p. 12-13.

50 La pseudonymisation est définie par l'article 4(5) du RGPD comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »

51 En amont de sa publication, le décret a fait l'objet d'avis, notamment celui de la CNIL qui a souligné le besoin d'informer individuellement la personne qui se fait vacciner tout comme celle qui reçoit un bon de vaccination quant au traitement de leurs données personnelles (délib. n° 2020-126, 10 déc. 2020, portant avis sur un projet de décret autorisant la création d'un traitement de données à

caractère personnel relatif à la gestion et au suivi des vaccinations contre le coronavirus SARS-CoV-2 (demande d'avis n° 20020767)). Pour sa part, le Comité consultatif national d'éthique (CCNE) a indiqué, dans un avis du 21 décembre 2020, que si « l'obligation d'une transparence et d'une rigueur des procédures vaccinales, et l'importance d'une pharmacovigilance réactive, nécessitent d'enregistrer des données » cet enregistrement ne doit pas « porter atteinte à l'anonymat qui protège les libertés individuelles ». Le Conseil souhaitant que le « dispositif de suivi informatique mis en place » fasse l'objet d'une attention particulière (CCNE, Enjeux éthiques d'une politique vaccinale contre le Sars-CoV-2, Réponse du CCNE à la saisine du ministre des Solidarités et de la Santé, 18 déc. 2020, p. 5).

52 Dans cette perspective, l'Union européenne œuvre pour la reconnaissance mutuelle des futurs certificats de vaccinations sous format électronique, v. Conseil de l'UE, Oral conclusions drawn by President Charles Michel following the video conference of the members of the European Council on 21 January 2021 (n° 34/21) ; eHealth Network, Guidelines on proof of vaccination for medical purposes – basic interoperability elements, 27 janv. 2021.

53 Cons. const., 13 nov. 2020, n° 2020-808 DC, Loi autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire.

54 Comité de contrôle et de liaison Covid-19, Pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie, avis du 15 sept. 2020, Paris, p. 9.

55 CE, avis n° 401 741, 20 déc. 2020, sur un projet de loi instituant un régime pérenne de gestion des urgences sanitaires.

56 Discours sur l'état de l'Union de la présidente Ursula Von der Leyen, 16 sept. 2020, <https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_20_1655>dernier accès le 17 février 2020.

57 Dir. (UE) n° 2019/1024 du Parlement européen et du Conseil, 20 juin 2019, concernant les données ouvertes et la réutilisation des informations du secteur public.

58 Règl. (UE) n° 2016/679 du Parlement européen et du Conseil, 27 avr. 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 (règlement général sur la protection des données).

59 Dir. (UE) n° 2019/1024 du Parlement européen et du Conseil, 20 juin 2019, concernant les données ouvertes et la réutilisation des informations du secteur public.

60 Dir. n° 2011/24/UE du Parlement européen et du Conseil, 9 mars 2011, relative à l'application des droits des patients en matière de soins de santé transfrontaliers, *JO* L 88, 4 avr. 2011, p. 45-65.

61 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-A-European-Health-Data-Space> dernier accès le 15 février 2021.

62 Commission européenne, *Livre blanc intelligence artificielle, Une approche européenne axée sur l'excellence et la confiance*, 19 févr. 2020, COM(2020) 65 final.

63 CESE, avis *n*° 2017/C 288/01, 31 mai 2017, sur l'intelligence artificielle : les retombées de l'intelligence artificielle pour le marché unique (numérique), la production, la consommation, l'emploi et la société.

64 Parlement européen, Projet de motion pour une résolution « on Automated decision-making processes : Ensuring consumer protection, and free movement of goods and services », 21 janv. 2020, n° 2019/2915 (RSP).

65 Le Parlement soutient les initiatives en faveur de l'IA à l'image de la création d'un espace européen des données de santé, PE, *Rapport contenant des recommandations à la Commission concernant un cadre d'aspects éthiques en matière d'intelligence artificielle, de robotique et de technologies connexes* (2020/2012(INL)), pt. 61.

66 Point K du rapport.

67 Point 135 du rapport.

68 Dir. (UE) n° 85/374/CEE du Conseil, 25 juill. 1985, relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux.

69 FRA, *Getting the future right – Artificial intelligence and fundamental rights*, Vienne, 14 déc. 2020.

70 R. T. Vought, *White House's memorandum on the regulation of AI applications*, Washington DC, 17 nov. 2020, M-21-06.

71 Conseil de l'Europe, Mise en place éventuelle d'un mécanisme de certification des outils et services d'intelligence artificielle dans le domaine juridique et judiciaire, étude de faisabilité réalisée par la Commission européenne pour l'efficacité de la justice, 8 déc. 2020, CEPEJ(2020)15Rev, p. 28.

72 La prochaine étape pour le Conseil de l'Europe est maintenant de mener une étude de faisabilité sur la numérisation des documents judiciaires. Conseil de l'Europe, Feuille de route du Groupe de travail sur la cyberjustice pour 2021 (CEPEJ-GT-CYBERJUST), 8 déc. 2020, CEPEJ(2020)14 REV.