Droit du numérique

Margo Bernelin, Jessica Eynard

CHRONIQUE NUMERIQUE N°15

Margo Bernelin
Jessica Eynard

De façon désormais classique, l'actualité dans le champ du numérique est très riche. Sans prétendre à l'exhaustivité, les auteures de cette chronique en proposent un panorama thématique (**I**) avant de se concentrer sur un sujet choisi, en l'occurrence l'usage du numérique en santé (**II**).

PANORAMA

Données personnelles.

Commission nationale de l'informatique et des libertés (CNIL)
La délibération de la CNIL en date du 10 février 2022 et qui porte sur l'outil d'analyse d'audience Google Analytics est remarquable. Dans cette affaire, la CNIL, en coopération avec ses homologues européens, a analysé les conditions dans lesquelles les données collectées dans le cadre de l'utilisation de cet outil étaient transférées vers les États-Unis et quels étaient les risques encourus pour les personnes concernées. A la suite de l'arrêt Schrems II de la Cour de justice de l'Union européenne du 16 juillet 2020, elle en conclut que la protection assurée outre-Atlantique n'est pas adéquate et que les mesures supplémentaires prises par Google ne suffisent pas à exclure la possibilité d'accès des services de renseignements américains aux données. Elle décide donc de mettre en demeure le gestionnaire de site web contrôlé de mettre en conformité le traitement relatif à la fonctionnalité Google Analytics avec le RGPD, en cessant, si nécessaire, de traiter des données à caractère personnel dans le cadre de la version actuelle de Google Analytics. D'autres procédures sont en cours et il faut s'attendre à de nouvelles décisions dans les mois à venir, tant à l'échelle nationale qu'européenne. On notera d'ailleurs qu'avec sa délibération, la CNIL rejoint la position de l'autorité de contrôle autrichienne qui s'était déjà prononcée sur l'outil Google Analytics dans une délibération du 22 décembre 2021 (accessible via le lien https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf).

Comité européen de la protection des données (CEPD)
1) Le 18 janvier 2022, le CEPD a publié, pour consultation, ses lignes directrices relatives au droit d'accès des personnes concernées par un traitement de données personnelles (Guidelines 01/2022 on data subject rights - Right of access). Selon lui, le périmètre du droit d'accès doit s'entendre largement et concerner l'ensemble des informations qui identifient ou qui permettent d'identifier directement ou indirectement une personne. En cela, il est plus étendu que le droit à la portabilité qui est restreint aux informations fournies par la personne elle-même. L'importance de la quantité de données concernées peut conduire à des difficultés d'identification des informations mais aussi de communication de celles-ci si bien que le CEPD propose des pistes à l'image d'un outil dédié qui serait aux mains de la personne concernée ou d'une communication échelonnée. Le Comité s'attache ensuite à tracer de façon stricte les frontières du droit d'accès, en indiquant que ce droit ne peut être limité par le responsable de traitement arguant d'efforts déraisonnables pour y faire droit ou par les parties

dans un contrat. Il apparaît que seuls trois fondements sont légitimes pour limiter ce droit : le cas où l'exercice du droit d'accès porterait atteinte aux droits des tiers, les demandes excessives ou manifestement infondées et les restrictions au droit d'accès provenant du droit national des États membres, conformément à l'article 23 du RGPD.

2) Le 22 février 2022, le CEPD a adopté des lignes directrices (Guidelines 04/2021 on Codes of Conduct as tools for transfers) visant à préciser les conditions dans lesquelles un code de conduite pouvait être considéré comme un outil approprié de transfert de données personnelles vers des pays n'offrant pas un niveau adéquat de protection. Il en ressort que le code de conduite doit être approuvé selon une procédure spécifique et être assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées. Le CEPD s'intéresse plus particulièrement à certaines clauses à intégrer au contrat ou à l'instrument contraignant choisi, lequel devrait mentionner :

- l'existence d'un droit, pour les personnes concernées dont les données sont transférées en vertu du code, de faire respecter les règles du code en tant que tiers bénéficiaires ;
- la question de la responsabilité en cas de violation des règles du code par un membre y adhérant qui se situe en dehors de l'espace économique européen. La personne concernée devrait pouvoir saisir l'autorité de contrôle et/ou la juridiction de son lieu de résidence ;
- l'existence d'un droit pour l'exportateur de faire valoir contre un importateur de données adhérant au code les règles prévues par le code, en tant que tiers bénéficiaire ;
- l'obligation de notification d'une violation du code dans des conditions particulières.

3) Outre les codes de conduite, la CEPD s'est intéressé à la certification comme moyen de transfert de données hors de l'Union dans des lignes directrices 07/2022 publiées pour consultation le 14 juin 2022, au sujet de la certification comme outil de transfert de données personnelles. Ces recommandations complètent des lignes directrices antérieures, notamment celles du 4 juin 2019 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement (1/2018). Ici, le CEPD s'attache à spécifier les obligations de l'exportateur des données, qui est considéré comme le responsable du traitement. Il précise et complète les critères de certification dont certains font suite à des arrêts de la Cour de justice (par ex., l'évaluation de la législation étrangère). Il revient enfin sur l'engagement contraignant et exécutoire d'appliquer des garanties appropriées qui accompagne la certification en indiquant qu'il doit *« inclure une garantie que l'importateur n'a aucune raison de croire que les lois et pratiques du pays tiers applicables au traitement en cause y compris les exigences de divulgation des données à caractère personnel ou les mesures autorisant l'accès des autorités publiques, l'empêchent de respecter ses engagements au titre de la certification et qu'il informera l'l'exportateur de tout changement pertinent dans la législation ou les pratiques à cet égard »* (point 51).

4) Le 14 mars 2022, le CEPD a consacré des lignes directrices à l'article 60 du Règlement général sur la protection des données (RGPD) et au mécanisme de coopération qu'il met en œuvre entre l'autorité chef de file et les autorités de contrôle nationales concernées (Guidelines 02/2022 on the application of Article 60 GDPR). Il précise les obligations qui incombent à ces acteurs qui doivent œuvrer pour parvenir à un consensus et s'adresser en temps utile les informations pertinentes, c'est-à-dire toutes les informations qui contribuent

directement ou indirectement à la conclusion de la procédure. L'autorité chef de file peut enjoindre aux autorités concernées qu'elles désignent, de mettre en œuvre une assistance mutuelle et des opérations conjointes. Elle est, quant à elle, tenue de soumettre un projet de décision à ces dernières et de prendre en considération leur point de vue. Conformément à l'article 60 du RGPD, le projet de décision peut faire l'objet d'une objection pertinente et motivée qui ouvre une nouvelle phase d'échanges entre l'autorité chef de file et les autorités de contrôle concernées. Cela peut aboutir au retrait de l'objection ou à la saisine du CEPD si l'autorité chef de file considère que l'objection n'est pas pertinente et motivée ou si elle refuse de la suivre. L'autorité chef de file peut également décider de retenir une objection, auquel cas elle doit soumettre un projet de décision modifié aux autorités de contrôle concernées qui pourront exprimer leur point de vue sur les amendements opérés. Dès lors qu'aucune objection n'est plus soulevée, les autorités de contrôle sont réputées être arrivées à un accord et le projet de décision devient contraignant pour le cas d'espèce uniquement.

5) Le 12 mai 2022, le CEPD a apporté des précisions sur l'utilisation de la reconnaissance faciale en matière pénale (Guidelines for public consultation 05/2022 on the use of facial recognition technology in the area of law enforcement). L'intérêt de ce document réside essentiellement dans ses trois annexes qui visent à permettre une évaluation pratique de la légalité des dispositifs de reconnaissance faciale mis en oeuvre. L'annexe I dresse un ensemble de points à considérer pour apprécier la sensibilité du mode d'utilisation de la reconnaissance faciale souhaité. L'annexe II contient des conseils pratiques à l'intention des autorités répressives qui souhaitent acquérir et exploiter un système de reconnaissance faciale. Elle s'intéresse aux différents acteurs impliqués et à leurs obligations respectives avant de dresser une liste des points de vigilance à traiter à chaque étape de la mise en œuvre d'un système de reconnaissance faciale. L'annexe III, enfin, expose six scenarii possibles dans lesquels un tel système est utilisé.

6) Toujours le 12 mai 2022, le CEPD a publié pour consultation publique des lignes directrices fixant une méthodologie en cinq étapes destinée à harmoniser les méthodes de calcul des amendes administratives adoptées par les autorités de contrôle nationales (Guidelines 04/2022 on the calculation of administrative fines under the GDPR). Ce document complète les lignes directrices que le CEPD avait adoptées sur l'application et la fixation des amendes administratives dans le cadre du RGPD et qui se concentraient sur les circonstances dans lesquelles infliger une telle amende (Lignes directrices sur l'application et la fixation des amendes administratives, WP253, 3 octobre 2017). Dans ce document, le CEPD fixe une méthodologie en cinq étapes.

Conseil d'Etat (CE)

Dans un arrêt du 26 avril 2022 (n°442364), le Conseil d'Etat a rejeté la requête formulée par l'association La Quadrature du Net au sujet de plusieurs dispositions du code de procédure pénale (alinéas 16 et 59 de l'article R. 40-26) qui autorisent l'enregistrement dans le traitement des antécédents judiciaires (TAJ) d'une « photographie comportant les caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale » concernant respectivement les personnes physiques mises en cause et les personnes physiques faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition. Dans son arrêt, le Conseil d'Etat valide le mécanisme légal mis en œuvre qu'il qualifie de « nécessité absolue » au motif notamment que, « eu égard au nombre de personnes mises en cause enregistrées dans ce traitement, qui s'élève à plusieurs millions, il est matériellement impossible aux agents compétents de procéder manuellement à une telle comparaison, de surcroît avec le même degré de fiabilité que celui qu'offre un algorithme de

reconnaissance faciale correctement paramétré ». Pour lui, les garanties qui entourent ce dispositif sont appropriées. Le doute à ce sujet est néanmoins légitime, notamment à la lumière des discussions en cours sur l'encadrement des systèmes d'intelligence artificielle recourant à la reconnaissance faciale dans le contexte de la proposition de règlement sur l'intelligence artificielle.

Cour de Justice de l'Union européenne (CJUE)

1) Dans une décision du 24 mars 2022 (X et Z c/ Autoriteit Persoonsgegevens, aff. C-245/20), la CJUE a considéré qu'une autorité de contrôle nationale était incompétente pour apprécier la conformité d'une mise à disposition temporaire, par des juridictions et au profit de journalistes, de pièces contenant des données personnelles qui sont issues d'une procédure juridictionnelle, aux règles posées par le RGPD, en application de l'article 55 paragraphe 3 de ce texte. Pour elle, le traitement consistant à fournir des informations personnelles à des journalistes dans le but de leur permettre de rendre compte du déroulement de la procédure juridictionnelle ou d'éclairer un aspect d'une décision rendue « se rattache clairement à l'exercice, par ces juridictions, de leur "fonction juridictionnelle", dont le contrôle par une autorité extérieure serait susceptible de porter atteinte, de manière générale, à l'indépendance du pouvoir judiciaire ».

2) Le 28 avril 2022 (aff. C-319/20), la CJUE a répondu à une question préjudicielle qui lui avait été posée dans le cadre d'un litige opposant la société Meta Platforms Ireland (Meta) à l'Union fédérale, association allemande de défense des intérêts des consommateurs. Il s'agissait de savoir si une association de protection des droits des consommateurs était recevable à agir sans mandat, ni même violation précisément identifiée des droits d'une personne concernée, sur le fondement de législations qui ne sont pas spécifiques au droit des données personnelles. La Cour répond par l'affirmative, ouvrant par là-même plus largement les possibilités d'actions de groupe en la matière.

Traitement de données personnelles et transport maritime

Le transport maritime fait l'objet d'une surveillance au sein de l'Union européenne depuis la directive 2002/59/CE relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information[1]. En France, cette surveillance passe par la mise en œuvre d'un traitement informatisé de données nommé « Trafic 2000 » qui vise notamment à surveiller le transport de marchandises dangereuses et polluantes par navires[2]. Pour ce faire, les données collectées ne concernent pas seulement les navires, cargaisons et escales, mais visent aussi les données des personnes présentes lors du transport maritime, à savoir les noms et prénoms du capitaine du navire, ceux des membres de l'équipage, des passagers ou encore des dockers. Certaines catégories de personnes font l'objet d'une collecte plus large de données. C'est le cas des membres d'équipage et des passagers des navires pour qui les déclarations doivent comprendre également le sexe, le cas échéant le grade ou la fonction, la nationalité, la date et le lieu de naissance, le type de pièce d'identité, le numéro de la pièce d'identité, le numéro de visa ou du permis de résidence ou encore des informations sur leur voyage s'ils sont passagers. Un arrêté en date du 25 février 2022 vient compléter ces éléments

[1]Directive 2002/59/CE du Parlement européen et du Conseil du 27 juin 2002 relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information.

[2] Voir l'arrêté du 19 mars 2012 portant création d'un traitement de données à caractère personnel relatif au suivi du trafic et à la sécurité maritimes dénommé « TRAFIC 2000 »

et autorise, à présent, la conservation des données des membres d'équipage et des passagers plus longtemps qu'auparavant, à savoir soixante jours au lieu de quinze[3].

Données de connexion

La saga sur la conservation des données de connexion continue[4]. La Cour de justice de l'Union européenne s'est à nouveau prononcée à ce sujet le 5 avril 2022, suivie par la Cour de cassation le 12 juillet 2022. Le Conseil constitutionnel procède quant à lui par à-coups.

1) Dans l'affaire ayant donné lieu à la décision du 5 avril 2022 (C-140/20, EU:C:2022:258), la Cour de justice devait apprécier la conformité au droit de l'Union de la loi irlandaise. En vertu de celle-ci, les fournisseurs de services de communications électroniques avaient conservé les données relatives au trafic et à la localisation afférentes à des appels téléphoniques d'une personne inculpée pour meurtre et rendu accessibles ces données aux autorités de police. La Cour applique notamment ici les principes dégagés dans ses arrêts du 6 octobre 2020, Privacy International (C-623/17, EU :C :2020 :790) et La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU :C :2020 :791). Elle rappelle que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques n'est pas autorisée aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique. Pour la Cour, seul l'objectif de sauvegarde de la sécurité nationale peut justifier que des mesures législatives prévoient la possibilité de recourir, pour une durée limitée, à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En matière de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique, la Cour fixe une liste de mesures de conservation qu'il est possible d'adopter, tout en posant le principe du respect de conditions matérielles et procédurales ainsi que la mise en œuvre de garanties effectives contre les risques d'abus pour les personnes concernées. L'utilisation d'un traitement centralisé des demandes d'accès effectuées par la police par un fonctionnaire de police, ne remplit par exemple pas ces exigences, notamment en termes d'indépendance et d'impartialité. Sur ce point, elle avait déjà jugé dans un arrêt du 2 mars 2021, Prokuratuur (C-746/18), que le droit de l'Union s'opposait à une réglementation nationale donnant compétence au ministère public, qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation.

2) Le 12 juillet 2022, c'est la Cour de cassation qui s'est prononcée sur la question de la conservation et de l'accès aux données de connexion. Par quatre arrêts (pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652), la chambre criminelle tire les conséquences des décisions de la Cour de justice de l'Union européenne. Elle aboutit à la conclusion que l'obligation de conservation généralisée et indifférenciée des données de connexion prévue par l'article L.34, III du CPCE, dans sa version antérieure à l'entrée en vigueur de la loi n° 2021-998 du 30 juillet 2021, n'est conforme au droit de l'Union que s'agissant de la répression des atteintes aux intérêts fondamentaux de la Nation et du terrorisme, incriminées aux articles 410-1 à 422-7 du code pénal et qui poursuivent l'objectif de sauvegarde de la sécurité nationale. Elle décide en outre que les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de

[3] Arrêté du 25 février 2022 portant modification de l'arrêté du 19 mars 2012 portant création d'un traitement de données à caractère personnel relatif au suivi du trafic maritime dénommé « TRAFIC 2000 »

[4] Voir *infra*, chronique « Preuve ».

procédure pénale ne sont pas conformes au droit de l'Union en ce que les réquisitions sont délivrées, en enquête de flagrant délit, par un officier de police judiciaire ou par un agent de police judiciaire agissant sous son contrôle, ou lors d'une enquête préliminaire, sur autorisation du procureur de la République, sans contrôle préalable par une juridiction ou une autorité administrative indépendante. Cette issue pose incontestablement des difficultés tant et si bien que la Cour de cassation publie un vade-mecum à destination des chambres de l'instruction dans sa note explicative des arrêts rendus le 12 juillet 2022 (https://www.courdecassation.fr/files/files/Communiqu%C3%A9s/Note%20explicative%20donn%C3%A9es%20de%20connexion%2012%20juillet%202022.pdf). Selon ce document, la chambre de l'instruction, si elle est saisie d'un moyen de nullité pris de la violation des exigences européennes, doit vérifier :

1) si le requérant est recevable à contester la régularité de la conservation et de l'accès à ses données de trafic et de localisation (question de la qualité pour agir) ;

2) si les données en cause ont été régulièrement conservées (finalité de sauvegarde de la sécurité nationale, possibilité de conservation rapide pour lutter contre la criminalité grave) ;

3) si l'accès a fait l'objet d'un contrôle indépendant préalable ;

4) si l'accès aux données de trafic et de localisation autorisé par le procureur de la République ou l'officier de police judiciaire a occasionné un grief au requérant. La chambre criminelle précise ici que « si l'accès aurait dû être refusé, la chambre de l'instruction doit prononcer la nullité des réquisitions en cause et des actes subséquents ».

3) On rappellera que la possibilité pour le procureur de la République ou, sur autorisation de celui-ci, de requérir des informations issues d'un système informatique ou d'un traitement de données nominatives édictée par l'article 77-1-1 du code de procédure pénale avait déjà été considéré comme non conforme à la Constitution dans une décision n°2021-952 du 3 décembre 2021 rendue par le Conseil constitutionnel répondant à une question prioritaire de constitutionnalité. Simplement, la date d'effet de cette inconstitutionnalité avait été repoussée au 31 décembre 2022. S'étant déjà prononcé sur ce texte, le Conseil a refusé de statuer de nouveau à ce sujet dans une affaire similaire le 25 février 2022 (décision n° 2021-974 QPC). On observera que la possibilité de réquisition des informations issues d'un système informatique ou d'un traitement de données nominatives prévue par l'article 60-1 du code de procédure pénale, dans sa rédaction résultant de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, a en revanche, après analyse des modalités d'application et de contrôle, été validée par le Conseil constitutionnel, de même que la mise à disposition d'informations prévues par l'article 60-2 du même code (décision n° 2022-993 QPC du 20 mai 2022). Enfin, le Conseil a considéré que la possibilité pour le juge d'instruction ou l'officier de police judiciaire commis par lui de requérir des informations issues d'un système informatique ou d'un traitement de données nominatives prévue à l'article 99-3 du code de procédure pénale, dans sa rédaction résultant de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, était constitutionnelle (décision n°2022-1000 QPC du 17 juin 2022). L'intervention d'un magistrat indépendant agissant dans un cadre strict présentant des garanties pour les droits et libertés individuels a fondé sa décision.

Enfin, le 25 février 2022, le Conseil constitutionnel s'est prononcé sur la constitutionnalité de l'article L. 34-1 du code des postes et des communications électroniques dans sa rédaction résultant de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la

sécurité nationale. Il a décidé de censurer cette disposition au motif « qu'en autorisant la conservation générale et indifférenciée des données de connexion, les dispositions contestées portent une atteinte disproportionnée au droit au respect de la vie privée » (décision n°2021-976/977 QPC du 25 février 2022).

Cookies

Faisant suite à une première vague de sanctions prononcées à la fin de l'année 2020 et en avril 2021 (décisions CNIL, formation restreinte, 18 novembre 2020, SAN-2020-009, Carrefour Banque ; 7 décembre 2020, SAN-2020-012, Amazon et SAN-2020-013, Google ; 27 juillet 2021, SAN-2021-013, Le Figaro) dont l'une avait déjà concerné la société Google, la CNIL a adopté deux délibérations le 31 décembre 2021 dans lesquelles elle sanctionne d'une amende administrative, assortie d'une injonction de se mettre en conformité sous astreinte de 100 000€ par jour de retard, la société Facebook Ireland Limited (délibération n°SAN-2021-024) à hauteur de 60 millions d'euros, et les sociétés Google LLC et Google Ireland Limited (délibération n°SAN-2021-023) à hauteur de 150 millions d'euros au motif, notamment, qu'il n'est pas permis aux utilisateurs de leurs services facebook.com, google.fr et youtube.com de refuser les cookies aussi facilement que de les accepter.

Dans le contexte du dépôt de traceurs, la CNIL a été confortée dans son rôle par plusieurs arrêts du Conseil d'Etat. Le premier, en date du 28 janvier 2022 (n°449209), valide les amendes d'une valeur de 100 millions d'euros qu'elle avait prononcées à l'égard de la société Google en décembre 2020. Dans cette décision, le juge administratif exclut l'application du système du guichet unique, donnant compétence à la juridiction du lieu de l'établissement principal du responsable du traitement, pour retenir la compétence de la CNIL en matière de dépôt de cookies dans l'équipement terminal d'un utilisateur. Il observe, entre autres, le non-respect par la société de ses obligations en matière de recueil du consentement pour considérer que les amendes prononcées ne sont pas disproportionnées eu égard aux bénéfices réalisés par Google grâce aux traceurs et à la position de cette entreprise en termes de parts de marché. Dans la lignée de cette décision, le Conseil d'Etat est intervenu pour valider la sanction de 35 millions d'euros prononcée à l'égard de la société Amazon, dans un arrêt du 27 juin 2022 (n°451423).

Contenus illicites/désinformation

1) Un accord de principe a été trouvé par les institutions de l'Union européenne au sujet de la proposition de règlement du 15 décembre 2020 relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, autrement appelée le DSA pour Digital Services Act. Ce texte conserve le principe d'une absence d'obligation de surveillance généralisée et de filtrage des contenus postés sur internet, tout en indiquant la possibilité pour un Etat d'exiger le maintien hors ligne de contenus précédemment considérés comme illicites (conformément à l'arrêt CJUE, Eva Glawischnig-Piesczek/Facebook Ireland Limited, 3 octobre 2019, C18/18) et en établissant un ensemble d'obligations échelonnées en fonction de l'activité et de la taille de l'acteur concerné. Le fournisseur de services intermédiaires ou d'hébergement, y compris les plateformes en ligne, les grandes plateformes en ligne et les très grands moteurs de recherche en ligne ne sont pas soumis aux mêmes obligations. Seuls les deux derniers doivent ainsi par exemple prendre des mesures de lutte contre les risques systémiques et participer financièrement à la lutte contre les contenus illicites, via des frais de supervision. La Commission européenne hérite ici d'un pouvoir de contrôle important, avec l'abandon notoire de la règle du pays d'origine. Dans sa

dernière mouture, le DSA apporte des éléments en lien avec les interfaces trompeuses (« dark patterns ») et la publicité ciblée à destination de personnes dont on peut raisonnablement penser qu'il s'agit de mineurs ou fondée sur du profilage permis par l'utilisation de données sensibles (art. 24 3.). Ces pratiques sont prohibées par principe. Concernant plus particulièrement les « dark patterns », ceux-ci sont définis comme « des pratiques qui, de manière significative, altèrent ou compromettent, de manière intentionnelle ou de fait, la capacité des destinataires du service à faire des choix ou à prendre des décisions autonomes et informées » (considérant 51b). En l'état du texte, il est possible de s'interroger sur les cas dans lesquels l'interdiction posée sera appliquée dès lors que le texte lui réserve les situations dans lesquelles le droit de la consommation (Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil, autrement appelée «directive sur les pratiques commerciales déloyales») et le droit des données personnelles (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, autrement appelé règlement général sur la protection des données) seront inapplicables. En outre, le texte exclut de la qualification de « dark patterns » les pratiques légitimes par exemple en matière de publicité, qui sont conformes au droit de l'Union. Le DSA admet par ailleurs l'utilisation de systèmes de recommandation mais pose un cadre légal en exigeant que les paramètres de ces systèmes soient connus de l'utilisateur qui doit pouvoir les modifier (art. 24a).

2) On notera par ailleurs les avancées faites en matière de désinformation, avec la signature le 16 juin 2022 par 34 adhérents d'un code européen de bonnes pratiques renforcé par rapport à celui de 2018, et qui deviendra contraignant pour ses signataires dans le cadre du DSA. Parmi les bonnes pratiques visées, on retiendra celles visant à démonétiser les fournisseurs de contenus de désinformation par le retrait des recettes publicitaires, à renforcer les mesures de transparence en matière de publicité politique, à assurer l'intégrité des services en luttant contre des comportements manipulatoires (faux-comptes, usurpation d'identité, …) ainsi qu'à responsabiliser les acteurs impliqués (utilisateurs, chercheurs, communauté de vérification des faits). Un Centre de transparence et une « task force » sont en outre créés de façon à assurer une visibilité des mesures prises et une durabilité du code dans le temps. D'autres codes de conduite devraient suivre.

3) La lutte contre les contenus illicites et la responsabilité des plateformes dans ce contexte a été illustrée en jurisprudence par un arrêt de la cour d'appel de Paris du 20 janvier 2022. Dans cette décision, la Cour confirme le jugement de première instance, aux termes duquel la société Twitter International Company est condamnée à communiquer aux parties adverses dans un délai de deux mois :

- « tout document administratif, contractuel, technique, ou commercial relatif aux moyens matériels et humains mis en oeuvre dans le cadre du service Twitter pour lutter contre la diffusion des infractions d'apologie de crimes contre l'humanité, l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle, l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que des atteintes à la dignité humaine ;

• le nombre, la localisation, la nationalité, la langue des personnes affectées au traitement des signalements provenant des utilisateurs de la plate-forme française de ses services de communication au public en ligne ;

• le nombre de signalements provenant des utilisateurs de la plate-forme française de ses services, en matière d'apologie des crimes contre l'humanité et d'incitation à la haine raciale, les critères et le nombre des retraits subséquents ;

• le nombre d'informations transmises aux autorités publiques compétentes, en particulier au parquet, en application de l'article 6.-I. 7 de la loi pour la confiance dans l'économie numérique (LCEN) au titre de l'apologie des crimes contre l'humanité et de l'incitation à la haine raciale ».

4) En matière de contenus terroristes, le règlement (UE) 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne est entré en application le 7 juin 2022. Il prévoit notamment une obligation de retrait et de blocage de tels contenus à la charge des fournisseurs de services d'hébergement, dans le délai d'une heure après avoir reçu une injonction de la part des autorités des États membres (art. 3 paragraphe 3).

En France, la proposition de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne a été adoptée. Elle a fait l'objet d'une saisine du Conseil constitutionnel le 29 juillet 2022 par plus de soixante députés.

Marchés numériques

La proposition de règlement européen du 15 décembre 2020 relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), autrement appelé le Digital Markets Act (DMA) arrive au bout du processus législatif avec une adoption prévue en septembre/octobre 2022. Ce texte a pour objet de contribuer au bon fonctionnement du marché intérieur en établissant des règles harmonisées garantissant que les marchés soient contestables et équitables dans le secteur numérique dès lors que des contrôleurs d'accès sont présents.

Il pose des obligations et interdictions clairement définies pour un nombre limité de fournisseurs transfrontières de services de plateforme essentiels qui servent de points d'accès majeurs aux entreprises utilisatrices pour atteindre les utilisateurs finaux. Ces fournisseurs ou « contrôleurs d'accès » englobent les entités qui répondent à trois critères cumulatifs :

- avoir un impact significatif sur le marché intérieur.
- fournir un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux utilisateurs professionnels d'atteindre les utilisateurs finaux.
- jouir d'une position solide et durable, dans leurs activités, ou jouiront probablement d'une telle position dans un avenir proche.

Les acteurs visés peuvent agir dans l'un des dix cœurs d'activité retenus par le texte, parmi lesquels on trouve par exemple les moteurs de recherche, les réseaux sociaux, les places de marché, les services de cloud, les services publicitaires, les navigateurs web, les assistants virtuels, les systèmes d'exploitation… La Commission européenne est ici le chef d'orchestre dans la désignation des contrôleurs d'accès.

De façon générale, le règlement renforce les obligations et interdictions applicables à tous les contrôleurs d'accès, en permettant au surplus à la Commission d'imposer des obligations supplémentaires au cas par cas, pendant l'enquête servant à la désignation d'une entreprise comme contrôleur d'accès. Une attention particulière a été portée à la combinaison des données personnelles collectées. L'article 5 pose à cet égard le principe d'une interdiction de combiner les données provenant des divers services du contrôleur d'accès ou des services tiers

sans le consentement de la personne concernée. Il est également imposé à ces acteurs de fournir une version de leurs services sans combinaison de données. Des avancées en matière d'interopérabilité sont notables, en particulier concernant les messageries en ligne, de même qu'au sujet des acquisitions prédatrices, avec une obligation d'information de tout projet d'acquisition d'acteurs fournissant des services de plateforme essentiels ou tout autre service dans le secteur numérique ou permettant la collecte de données (art. 14). A défaut de respecter les obligations et interdictions posées par le texte, les contrôleurs d'accès s'exposent à être condamnés à des amendes allant jusqu'à 10 % de leur chiffre d'affaires mondial. En cas de récidive sur une même infraction, l'amende peut monter jusqu'à 20 %. Aucune amende plancher n'a, en revanche, été retenue à l'issue des négociations.

Stratégie européenne pour les données

Dans la période écoulée, deux textes qui relèvent de la stratégie de la Commission européenne en matière de données doivent être mis en lumière.

1) Le premier, connu sous le nom de règlement sur la gouvernance des données ou DGA pour Data Governance Act (Règlement (UE) 2022/868 du Parlement européen et du Conseil portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724) a été adopté le 30 mai 2022. Il vise à amplifier la réutilisation de données détenues par des organismes du secteur public, à permettre l'accès aux données détenues par les acteurs privés assurant un service de partage et à assurer l'accès par les acteurs publics aux données détenues par les entreprises privées lorsque cela s'impose pour protéger l'intérêt général. Ce dernier cas renvoie au terne utilisé dans le DGA d' « altruisme » en matière de données. Le régime mis en place en matière d'altruisme ne crée pas d'obligation pour les entreprises privées de partager leurs données mais les y incite en leur fournissant des garanties contre toute réutilisation qui pourrait leur porter préjudice. Le texte édicte par ailleurs la création d'un comité européen de l'innovation dans le domaine des données sous la forme d'un groupe d'experts dont les missions relèvent principalement du conseil et de l'assistance à l'égard de la Commission européenne. Il est également attendu de lui qu'il propose des lignes directrices pour des espaces européens communs de données et qu'il facilite les collaborations entre autorités compétentes et entre États membres.

2) Le second texte, connu sous le nom de Data Act ou Règlement sur des règles harmonisées relatives à l'accès équitable aux données et à leur utilisation équitable, n'est encore qu'au stade de proposition. Il a été publié le 23 février 2022 avec le but de « garantir l'équité dans la répartition de la valeur des données entre les acteurs de l'économie fondée sur les données et de favoriser l'accès aux données et leur utilisation ». Cinq objectifs spécifiques sont énumérés, à savoir : 1) faciliter l'accès aux données et leur utilisation par les consommateurs et les entreprises, tout en préservant les incitations à investir dans les moyens de générer de la valeur au moyen de données ; 2) Prévoir l'utilisation, par les organismes du secteur public et les institutions, agences ou organes de l'Union, des données détenues par les entreprises dans certaines situations où il existe un besoin exceptionnel de données ; 3) Faciliter le passage entre les services en nuage et les services de périphérie ; 4) Mettre en place des garanties contre le transfert illicite de données sans notification par les fournisseurs de services en nuage ; 5) Prévoir l'élaboration de normes d'interopérabilité pour les données à réutiliser entre secteurs.

Le texte pose l'obligation de sécuriser les données générées par l'utilisation de produits ou de services connexes, sachant que le produit est défini comme « un bien corporel meuble, y compris lorsqu'il est incorporé dans un bien immeuble, qui obtient, génère ou recueille des

données concernant son utilisation ou son environnement, et qui est en mesure de communiquer des données par l'intermédiaire d'un service de communications électroniques accessible au public et dont la fonction première n'est pas le stockage et le traitement de données » (internet des objets) et le service connexe comme « un service numérique, y compris un logiciel, qui est intégré dans un produit ou interconnecté avec un produit de telle sorte que son absence l'empêcherait d'exercer l'une de ses fonctions ». Il impose que l'accès à ces données et leur utilisation soit facile pour les détenteurs des produits et bénéficiaires des services connexes qui peuvent exiger du détenteur des données qu'il les mette gratuitement à disposition d'un tiers. Dans ce cas, le Data Act prévoit des conditions équitables raisonnables, non discriminatoires et transparentes de mise à disposition des données et l'existence d'une compensation raisonnable. Le chapitre IV est consacré aux clauses contractuelles abusives relatives à l'accès aux données et à leur utilisation entre entreprises. Aux termes de l'article 13, « une clause contractuelle est abusive si elle est d'une nature telle que son utilisation s'écarte largement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation de celles-ci, ce qui est contraire à la bonne foi et à la loyauté ». Cette définition est complétée d'une liste de clauses considérées ou présumées abusives. Le chapitre V s'attache à poser les règles en matière de mise à disposition par les entreprises de données au profit des organismes du secteur public et institutions, des agences ou des organes de l'Union sur le fondement de besoins exceptionnels. Le texte précise les cas dans lesquels un tel besoin est réputé exister. Les demandes de données doivent être proportionnées, indiquer clairement l'objectif à atteindre et respecter les intérêts de l'entreprise qui met les données à disposition. Par la suite, le Data Act pose des exigences en termes d'interopérabilité applicables aux fournisseurs de services et aux opérateurs d'espaces de données et en termes de contrats intelligents. Il encadre aussi les transferts internationaux de données non personnelles. On notera en dernier lieu que, dans le souci de ne pas interférer avec les droits des entreprises et des consommateurs d'accéder aux données, de les utiliser les données et de les partager, la proposition prévoit que le droit *sui generis* du producteur d'une base de données ne s'applique pas aux bases de données contenant des informations obtenues ou générées par l'utilisation d'un produit ou d'un service connexe.

<u>Protection des mineurs en ligne.</u>

Nouvelle stratégie européenne pour un internet mieux adapté aux enfants.

Dans une communication du 11 mai 2022 (COM(2022) 212 final), la Commission européenne entend tracer les lignes de la future législation visant à protéger les enfants et les jeunes en ligne et à les former à cet environnement, en développant leurs compétences et en leur donnant les moyens de maîtriser leur vie numérique et d'en profiter en toute sécurité.

Cette nouvelle stratégie propose des actions s'articulant autour de trois piliers :

1. des expériences numériques sûres pour protéger les enfants et l'amélioration de leur bien-être en ligne grâce à un environnement numérique sûr et adapté à leur âge,;
2. l'autonomisation numérique permettant aux enfants d'acquérir les aptitudes et les compétences nécessaires pour faire des choix sains et s'exprimer de manière sûre et responsable dans l'environnement en ligne ;
3. la participation active et le respect des enfants en leur permettant d'avoir voix au chapitre dans l'environnement numérique..

Pour chacun de ces piliers, la Commission précise les actions qu'elle entend mener et celles qu'elle invite les États membres et les entreprises du secteur concerné à prendre.

Proposition de règlement européen établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants

Une nouvelle proposition de règlement (COM(2022) 209 final) a été présentée le 11 mai 2022, en même temps que la stratégie pour un internet mieux adapté aux enfants. Elle impose aux fournisseurs de services d'hébergement ou de communications interpersonnelles de procéder à une évaluation des risques d'utilisation à mauvais escient de leurs services aux fins de la diffusion de matériel connu ou nouveau relatif à des abus sexuels sur enfants ou de la sollicitation d'enfants et de prendre des mesures d'atténuation de ces risques. Les boutiques d'application logicielles se voient aussi imposer des obligations d'évaluation des services fournis. La proposition comprend des obligations ciblées imposant à certains fournisseurs de détecter lesdits abus, de les signaler, de retirer ou rendre inaccessible le matériel relatif à des abus sexuels sur enfants en ligne, ou de le bloquer lorsqu'on le leur enjoint. Pour exécuter leur obligation de détection, les acteurs concernés installent et exploitent en particulier des technologies permettant de détecter la diffusion de matériel connu ou nouveau relatif à des abus sexuels sur enfants ou la sollicitation d'enfants. Ces technologies doivent être efficaces, fiables, ne pas permettre de collecter des informations autres que celles qui sont strictement nécessaires pour détecter des schémas révélateurs de la diffusion de matériel connu ou nouveau relatif à des abus sexuels sur enfants ou la sollicitation d'enfants, conformes à l'état de la technique dans le secteur et être les moins intrusives en ce qui concerne l'incidence sur les droits des utilisateurs à la vie privée et familiale. Leur utilisation doit être entourée de garanties. Malgré cela, on peut s'interroger sur la compatibilité de l'obligation de détection avec le principe d'absence de surveillance généralisée et indifférenciée des contenus en ligne et, par suite, sur le respect de certains droits et libertés fondamentaux. Quant à l'obligation de retrait, elle doit être exécutée dès que possible à la suite d'une injonction et au plus tard dans les 24 heures de sa réception (art. 14).

Outre des obligations à la charge des fournisseurs de services d'hébergement ou de communications interpersonnelles, la proposition prévoit en particulier « la création d'un nouveau centre européen pour prévenir et combattre les abus sexuels commis contre des enfants, qui faciliterait la détection, le signalement et la suppression des matériels d'abus sexuels sur enfants en ligne, fournirait un soutien aux victimes et constituerait un pôle de connaissances, d'expertise et de recherche sur les questions liées à la prévention contre les abus sexuels sur enfants en ligne et à la lutte dans ce domaine »[5].

Sécurité

Identification électronique dans le champ de la santé : Il était attendu ! L'arrêté du 28 mars 2022 approuve le référentiel de l'Agence du Numérique en Santé (ANS) relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé. Le référentiel doit, par le respect de normes techniques, permettre d'assurer la sécurité et la confidentialité des données de santé grâce à la vérification des accès à ces dernières. Le référentiel en question se divise en trois volets dédiés aux acteurs pouvant accéder à des données de santé dans le cadre du soin, à savoir : les professionnels personnes physiques, les professionnels personnes morales et les usagers. Le processus de rédaction et de concertation menant à l'adoption du document s'est étalé sur plusieurs mois afin de « trouver le juste équilibre entre, d'une part, la nécessaire sécurité dans le traitement des données de santé et, d'autre part, la réalité des usages par les professionnels qui prennent en

[5] Communication du 11 mai 2022, Une décennie numérique pour les enfants et les jeunes : la nouvelle stratégie européenne pour un internet mieux adapté aux enfants, COM(2022) 212 final, p. 4.

charge les patients »[6]. Aussi, les règles adoptées et approuvées ne cherchent pas à alourdir le cahier des charges des fournisseurs de services numériques en santé ou des professionnels de la santé, mais bien à proposer un cadre technique sécurisé permettant la connexion aux outils techniques de lecture et de partage de données de santé, comme une plateforme de prise de rendez-vous, un logiciel interne à un établissement de soin ou encore une plateforme de consultation d'examens biologiques. Les trois volets du référentiel fixent, pour chacun des utilisateurs visés, l'état de l'art en la matière ainsi que des règles de natures diverses pour assurer la sécurité des données.

Sécurité informatique de l'État et des établissements publics

La sécurité informatique est bien au cœur de l'actualité récente. Le décret du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics en est une illustration dans le champ réglementaire[7]. Le texte impose à chaque ministère de nommer un fonctionnaire dédié à la sécurité informatique, lequel aura la tâche de s'assurer de l'application des règles de sécurité informatique applicables aux systèmes d'informations et aux communications. Il devra également rapporter à l'Agence nationale de sécurité des systèmes d'information tout incident de sécurité. Chaque ministre devra également nommer une autorité responsable de la sécurité informatique. Le décret vient imposer une homologation dans ce champ, c'est-à-dire « une décision formelle prise par l'autorité qualifiée en sécurité des systèmes d'information ou par toute personne à qui elle délègue cette fonction. Elle atteste que les risques pesant sur la sécurité ont été identifiés et que les mesures nécessaires pour maîtriser ces risques sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'autorité qualifiée en sécurité des systèmes d'information ». Enfin le décret précise que « le dirigeant exécutif d'un établissement public de l'État est responsable de la sécurité numérique des systèmes d'information et de communication de cet établissement ». Le décret permet de créer un maillage et des procédures propices à déceler les failles de sécurité et à assurer la protection des outils informatiques des ministères et de tout établissement public, ce qui inclut, par exemple, les centres hospitaliers.

Directive NIS 2 (directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union)

Le 22 juin 2022, les représentants des États membres ont validé la version de la directive NIS 2 arrêtée par le Conseil de l'Union européenne et le Parlement européen. Le parcours débuté le 16 décembre 2020 avec la proposition de directive de la Commission européenne est ainsi sur le point de toucher à sa fin. Une fois définitivement adopté, ce texte remplacera l'actuelle directive NIS relative à la sécurité des réseaux et des systèmes d'information (aussi appelée SRI pour Sécurité des Réseaux et des systèmes d'Information). Les États membres auront 21 mois pour procéder à la transposition dans leur droit interne. Prenant en compte les critiques formulées à l'égard du texte précédent, la directive NIS 2 vient moderniser « le cadre juridique existant en tenant compte de la numérisation accrue du marché intérieur ces dernières années et de l'évolution du paysage des menaces en matière de cybersécurité ».

Internet de confiance

L'Union européenne et ses partenaires internationaux ont proposé une déclaration visant à promouvoir les principes d'un internet de confiance, intitulé Déclaration pour le futur de l'internet

[6] ANS (https://esante.gouv.fr/espace-presse/un-grand-pas-pour-la-securite-et-les-usages-du-numerique-en-sante-publication-du-referentiel-sur-lidentification-electronique)

[7] https://www.legifrance.gouv.fr/download/pdf?id=K8XwN_zbqoVJla0rgPOiw3B0La5rYk6ys5dm_FwTPZs=

(file:///C:/Users/Jessica/Downloads/Declaration_for_the_Future_for_the_Internet_Launch_Event_Signing_Version_FINAL_20220428_UP5Fn1plmtpsmAPVJW1rqEkZL8_86262.pdf).
Parmi ces principes, peuvent être cités :

- le respect des droits de l'homme et des libertés fondamentales dans l'environnement en ligne ;
- le principe d'un internet global, inclusif et accessible par tous ;
- la mise en place d'un écosystème numérique de confiance, fondé sur la coopération , le respect du droit à la vie privée et à la protection des données personnelles, un accès aux données compatibles avec la réglementation européenne par les Etats membres…
- la mise en œuvre d'une gouvernance de l'internet multipartite.

FOCUS

L'USAGE DU NUMERIQUE SANTE

La santé est un champ qui met en lumière les visions concurrentes de l'usage d'outils numériques : un usage voulu mais également craint. Ainsi, l'actualité juridique est souvent faite de normes soutenant le déploiement du numérique (**A**) mais aussi de réflexions ou de nouvelles règles visant l'accompagnement de ce développement, voire un encadrement contraignant (**B**).

I - Soutenir le déploiement d'outils numériques

Quelle que soit l'échelle envisagée l'usage d'outils numériques dans le champ de la santé, et plus particulièrement pour le soin, fait l'objet d'un engouement particulier soutenu par les pouvoirs exécutif et législatif. En effet, qu'il s'agisse des politiques de santé (**1**) ou de la médecine de ville (**2**), le numérique est pensé comme un atout au service des pouvoirs publics mais aussi des patients, comme en témoigne l'actualité récente.

A - Numérique et santé publique

Remis au Ministre des solidarités et de la santé, le rapport Chauvin intitulé « Dessiner la santé publique de demain », fait la part belle au numérique et à ses multiples facettes[8]. Loin d'être un rapport d'information quelconque, il a vocation à être le fil conducteur d'une

« évolution en profondeur de l'organisation du système de santé publique français » (p.1) dont le numérique sera l'un des moteurs. Pour appuyer cette vision, le rapport se fonde notamment sur le retour d'expérience de la gestion de l'épidémie Covid-19 dans laquelle les outils numériques se sont révélés nécessaires, l'analyse de données massives et l'utilisation d'application de contact tracing ayant sauvé des vies, bien que l'auteur n'approfondisse pas la question de la mesure du phénomène. Le rapport préconise alors « d'investir dans le numérique en santé pour renforcer les connaissances en santé, la pertinence des interventions et la confidentialité des données ». Sur ce terrain, déjà largement défriché par les pouvoirs exécutif et législatif ces dernières années, le rapport propose trois actions :

- « Améliorer la collecte, la gestion et l'exploitation des données de santé

[8] Pr Franck Chauvin, Dessiner la santé publique de demain, 4 mars 2022.

- Développer la modélisation, l'anticipation et la prospective en santé au service des décideurs et de la population
- Développer le numérique comme outil d'intervention au plus près du terrain ».

Concernant la collecte des données de santé, le rapport insiste sur sa nécessité (p.17). Sans dire un mot de la spécificité de la collecte et du traitement des données de santé et des risques associés, notamment ceux pesant sur la vie privée, le rapport indique que la confiance « des populations passe par des conditions d'accès aux données simples et effectives et par des garanties de sécurité encadrant leur conservation et leurs usages ». Ainsi, c'est la sécurité, pensée comme un simple objectif technique, qui permettra l'adhésion de la « population », les droits individuels n'étant pas envisagés comme pouvant jouer un rôle ici.

Central pour les prochaines politiques de santé, ce rapport suggère donc l'amélioration du traitement des données de santé, passant par de nouvelles actions : soutien à la création de bases de données de santé, à la sécurisation et au partage de ces dernières (p.40) :

Le rapport donne le ton et la réalisation des objectifs de ce rapport passera par la modification ou la création de nouveaux traitements automatisés de données personnelles lesquels devront alors prendre en compte les droits des personnes concernées par ces derniers.

B - Numérique et médecine de ville

Les pouvoirs publics voient également dans le numérique un atout pour la médecine de ville et notamment pour permettre la prise en charge des patients nécessitant un rendez-vous rapidement avec un professionnel de santé. C'est ainsi, que la « Plateforme numérique du Service d'accès aux soins » a enfin été créée de manière pérenne grâce à la parution d'un décret très attendu[9]. En effet, dès septembre 2019, la Ministre des solidarités et de la santé avait annoncé le financement d'une plateforme en ligne et numérique d'accès aux soins devant permettre de désengorger les urgences en réorientant les patients nécessitant des soins courants vers la médecine de ville[10]. Ce service d'accès aux soins (SAS) a d'abord été lancé sous forme d'expérimentation pour offrir un service téléphonique conjointement avec les services du SAMU afin de réorienter les patients. Aujourd'hui, c'est une plateforme numérique qui s'ajoute à ce service téléphonique, grâce à un décret du 21 mars dernier qui autorise le traitement de données personnelles pour le fonctionnement du tout. Les données concernées sont celles des professionnels de santé qui pourraient être disponibles pour des soins non programmés. Leurs noms, coordonnées mais aussi spécialités et modalités d'exercice sont alors traités par la plateforme[11] tout comme leurs créneaux disponibles. Les patients potentiels peuvent donc joindre par téléphone le SAMU. À l'autre bout de la ligne, les services de médecine d'urgence pourront, si cela s'avère pertinent, prendre rendez-vous pour le patient, auprès d'un professionnel de santé en ville et éviter alors un passage aux Urgences de l'hôpital. La plateforme ne semble pas pour autant collecter les données des patients, si on se fie à la lecture du décret et des différents documents d'information.

Au-delà de la prise de rendez-vous, le numérique a également été identifié par la Convention pharmaceutique comme un enjeu justifiant une prise en charge par l'Assurance Maladie. Approuvée par un arrêté du 31 mars 2022, la Convention nationale organisant les

[9] Décret n° 2022-403 du 21 mars 2022 portant création d'un traitement automatisé de données à caractère personnel dénommé « Plateforme numérique du Service d'accès aux soins »

[10] Ministère des solidarités et de la santé, *Pacte de refondation des urgences*, 9 septembre 2019 (Mesure n°1).

[11] Article 2 du décret ; Agence du numérique « Projet PTF digitale SAS Spécifications techniques d'interopérabilité INT_R01 » 2022.

rapports entre les pharmaciens titulaires d'officine et l'Assurance maladie s'intéresse, en effet, en détail aux outils numériques[12] et introduit « la rémunération sur objectifs pour le développement du numérique en santé et l'amélioration de l'accès aux soins » (article IX). Selon le texte de la Convention : « l'alimentation de l'espace numérique en santé du patient, le recours aux logiciels d'aide à la dispensation certifiés, l'utilisation de la messagerie sécurisée, la bascule vers la e-prescription, et l'usage de l'application carte Vitale sont autant d'évolutions majeures qui sont intégrées dans une nouvelle rémunération sur objectifs pour le développement du numérique en santé et l'amélioration de l'accès aux soins ». Cette incitation par la rémunération se cristallise notamment sur l'annotation du dossier médical partagé ou du dossier pharmaceutique au sein de l'Espace numérique de santé du patient lors du passage à l'officine. Cette incitation nouvelle ancrée dans la Convention pharmaceutique pourrait permettre d'assurer le succès, tant espéré par les pouvoirs publics, du tout nouvel Espace numérique de santé.

Si le numérique est connoté positivement en santé, il faut également l'objet de réflexions quant à sa régulation.

II - Encadrer le déploiement d'outils numériques en santé

Les réflexions sur le déploiement d'outils numériques en santé ne visent pas simplement leur déploiement et les règles permettant de soutenir les chantiers en cours, mais concernent également son encadrement. Récemment ce sont à la fois des normes de droit souple (1) et des règles déontologiques qui ont fait l'objet de discussions (2).

A - Le droit souple pour encadrer le numérique en santé

Arrivée à la tête du Conseil de l'Union européenne, la France avait annoncé son intention de mobiliser ses partenaires européens sur l'usage d'outils numériques en santé. À cet égard, le dossier de presse de près d'une trentaine de pages indique que : « Notre avenir en santé s'appuiera sans nul doute sur le numérique en santé, et en collaboration au sein de l'Union européenne. La crise que nous traversons nous a montré combien ces usages étaient pertinents et se traduisaient par des services concrets pour le citoyen. C'est précisément ce que l'Europe souhaite faciliter avec l'espace européen de données de santé. Nous avons aussi pu observer au cours de ces derniers mois toute la pertinence de cet échelon européen que ce soit pour assurer le continuum de soins que dans la prévention, la politique publique ou la recherche »[13]. Aussi, les échanges et événements se sont multipliés sur ce thème et ont inclus la rédaction de principes éthiques. Au nombre de 16, ces derniers ont été adoptés en février 2022[14] par le E-Health Network, c'est-à-dire par les représentants des États membres en charge du numérique en santé. Ces 16 principes doivent fixer le cadre des prochaines évolutions législatives nationales et européenne. Ils sont déclinés en 4 objectifs :

- « inscrire le numérique en santé dans un cadre de valeurs humanistes ;
- donner la main aux personnes sur le numérique et leurs données de santé ;
- développer un numérique en santé inclusif ;
- mettre en œuvre un numérique en santé écoresponsable ».

[12] https://www.legifrance.gouv.fr/jorf/texte_jo/JORFTEXT000045538155
[13] Ministère des solidarités et de la santé, « Numérique en santé en France Stratégie dans le cadre de la Présidence Française du Conseil de l'Union Européenne Dossier de presse », 27 janvier 2022, p.1.
[14] < https://presidence-francaise.consilium.europa.eu/media/zp2jt3up/european-ethical-principles-for-digital-health_fr_eng.pdf >

L'originalité du document est qu'il ne se borne pas à souligner l'apport du numérique en santé et de poser les bases de son encadrement. En effet, il insiste également sur la nécessaire prise en charge physique des patients, le numérique ne venant qu'en soutien. En ce sens, le premier principe est ici intéressant ; il indique que « le numérique en santé complète et optimise les pratiques de santé en effectuées en présentiel ».
L'information des personnes face au déploiement du numérique en santé est également envisagée d'une manière renouvelée. Ainsi, il ne s'agit pas simplement d'informer les patients quant au traitement de leur données personnelles, mais plus largement d'apporter une information individuelle et plus généraliste sur les bénéfices et limites du numérique en santé (principe 2). Dans cette même veine, les principes prônent l'autonomie individuelle face au numérique en santé avec notamment la possibilité de pouvoir paramétrer soi-même ses interactions avec les outils (principe 3) ou encore la portabilité facilitée des données de santé (principe 6). Le document tente de ne pas oublier pour autant la fracture numérique qui frappe de nombreux patients, les éloignant de ces outils. Les principes promeuvent alors des formations individuelles (principe 11) et proposent que les outils numériques soient simples et intuitifs (principe 10) en incluant si besoin est une assistance humaine (principe 12). Enfin, le texte comprend quatre principes visant à réduire au maximum l'empreinte énergétique de ces outils numériques.
Eu égard aux thématiques abordées, ces principes méritent l'attention et, à l'heure où sont rédigées ces lignes, des travaux sont menés par le E-Health Network afin d'en proposer une mise en œuvre.

Si le droit souple offre une illustration intéressante des moyens d'encadrer le numérique par une approche éthique, la déontologie semble également fournir une piste.

B - Les règles déontologiques pour encadrer le numérique

Dans son bulletin spécial dédié au numérique en santé, l'Ordre des médecins propose sa vision de l'usage d'outils numériques[15]. Le point de vue de l'Ordre sur les évolutions numériques, et notamment sur l'espace numérique de santé individuel des Français, est positif : « les outils numériques sont au service du médecin dans son exercice et sa relation avec les patients et devront le rester ». Toutefois, le Conseil de l'Ordre note que le numérique soulève des enjeux particuliers eu égard au principe de libre choix du médecin, au secret professionnel, à l'indépendance professionnelle ou encore à la liberté de prescription. Se pose donc la question de l'encadrement par la norme déontologique de ces outils et des nouvelles pratiques et de l'opportunité, mise en lumière par la Feuille de route du Numérique en santé, de créer un code de « e-déontologie ». Après réflexion, cela n'est pas le chemin retenu par l'Ordre. En effet, il apparait « après examen de chaque article au prisme du numérique, que le code n'exige pas de réforme approfondie. Il est adapté au développement du numérique en santé, sous réserve d'en faire une lecture souple, une interprétation ouverte. Il est clair que le numérique bouge les lignes, mais ce sont surtout l'organisation des soins et les pratiques professionnelles qui sont bousculées »[16]. Aussi l'Ordre fait-il le choix d'adapter les règles existantes, notamment grâce aux commentaires des articles du code de déontologie, lesquels précisent le sens de ces derniers[17]. Par ailleurs, le Conseil de l'Ordre a fait le choix d'introduire un article spécifique relatif à l'e-santé, dont le contenu n'a pas encore été révélé. La méthode retenue par l'Ordre a le mérite de permettre une adaptation rapide des règles

[15]Ordre des médecins, Santé : La révolution Numérique, Bulletin spécial, janvier 2022, https://www.conseil-national.medecin.fr/publications/bulletins-lordre-medecins/medecins-special-revolution-numerique
[16] p. 14.
[17] p.17.

déontologiques aux outils et pratiques numériques. En effet, la publication de ces commentaires, sur le site internet de l'Ordre, est beaucoup plus rapide que l'adoption d'un décret pour toute modification du code. Néanmoins, le cadre posé restera souple, voire trop souple, les organes d'interprétation du droit, comme les juges, n'ayant pas l'obligation de se référer aux commentaires pour appliquer la règle. Aussi, il faudra évaluer la méthode au fil de l'eau pour la modifier si besoin.