IA & Stratégie européenne de la donnée

IA Act,

Data Governance Act, Data Act,

European Health Data Space

Eléonore Scaramozzino

Avocat Constellation Avocats

constellation • law

SOMMAIRE

IA & Stratégie européenne de la donnée

IA Act, Data Governance Act, Data Act, European Health Data Space

Par Eléonore Scaramozzino, Avocat, Constellation Avocats

Version du 15.01.2024

Dans le cadre de sa stratégie numérique, l'UE a souhaité réglementer les systèmes d'Intelligence Artificielle. **L'IA Act** deviendra la première régulation des systèmes d'Intelligence artificielle au monde. Elle est fondée sur une approche basée sur les risques. Les systèmes d'IA à risque inacceptable représentent une menace pour les personnes et seront interdits. Certaines exceptions peuvent être autorisées à des fins d'application de la loi. Les systèmes d'IA qui ont un impact négatif sur la sécurité ou les droits fondamentaux seront considérés comme à haut risque et seront divisés en deux catégories : ceux qui sont utilisés dans les produits relevant de la législation de l'UE sur la sécurité des produits, et ceux relevant de domaines spécifiques qui devront être enregistrés dans une base de données de l'UE. Tous les systèmes d'IA à haut risque seront évalués avant leur mise sur le marché et tout au long de leur cycle de vie. Les modèles d'IA à usage général à fort impact susceptibles de présenter un risque systémique, tels que le modèle d'IA plus avancé GPT-4, devraient faire l'objet d'évaluations approfondies et signaler tout incident grave à la Commission. Les systèmes d'IA à risque limité doivent respecter des exigences de transparence minimales qui permettraient aux utilisateurs de prendre des décisions éclairées. Après avoir interagi avec les applications, l'utilisateur peut alors décider s'il souhaite continuer à l'utiliser. Les

utilisateurs doivent être informés lorsqu'ils interagissent avec l'IA. En juillet 2023, le Parlement européen a intégré l'IA générative, comme ChatGPT, dans la réglementation de l'IA, en lui imposant des exigences de transparence.
En décembre 2023, le Parlement européen et le Conseil affichaient des divergences sur le champ d'application de la régulation des systèmes d'IA, et notamment sur la régulation des modèles de fondation par des règles contraignantes, et les exceptions aux interdictions. Le gouvernement français était favorable à une autorégulation des modèles de fondation. Le 8 décembre, les négociateurs sont parvenus à un accord provisoire sur la législation sur l'IA. Ces règles visent à protéger contre les risques liés à l'IA tout en encourageant l'innovation.

Cependant, le développement des systèmes d'IA nécessite un accès aux données pour créer de nouveaux services et pour entraîner ces systèmes d'IA. La Commission européenne a présenté en février 2020 sa stratégie européenne de la donnée, pour créer un marché unique de la donnée. Cette stratégie repose sur deux règlements : le Data **Governance Act** et le **Data Act,** qui visent à établir un marché unique des données facilitant leurs échanges et des espaces de données sectoriels, dont l'European Health Data Space (EHDS). Le règlement sur la gouvernance des données, le **Data Governance Act**, est entré en vigueur en septembre 2023. Il vise à créer les processus et les structures destinées à faciliter le partage de données par les entreprises, les particuliers et le secteur public. Il est complété par le règlement sur les données, **Data Act** vise à garantir l'équité dans le monde numérique, stimuler le développement d'un marché des données concurrentiel, et favoriser l'innovation. A cet effet, il instaure de nouvelles règles d'accès et d'utilisation des données générées dans l'UE dans tous les secteurs économiques afin de faciliter le partage des données en particulier des données industrielles. Sa mise en application est prévue pour le 11 septembre 2025. Le 3 mai 2022, la Commission a adopté une proposition de règlement relatif à l'espace européen des données de santé (EHDS). L'objectif est de garantir l'accès des personnes physiques à leurs données électroniques à caractère personnel et leur contrôle sur celles-ci (utilisation primaire), et d'établir un cadre pour la réutilisation des données dans l'ensemble de l'Union (utilisation secondaire). Le Parlement européen et le Conseil peuvent à présent engager les négociations interinstitutionnelles.

Focus sur l'EU IA ACT : accord Conseil –Parlement européen

Un accord sur la régulation des systèmes d'Intelligence Artificielle visant à garantir les droits fondamentaux, l'Etat de droit et la durabilité environnementale sont protégés contre les risques liés à l'IA, tout en encourageant l'innovation. Les règles établissent des obligations relatives au niveau de risque et d'impact que l'IA peut générer. La définition d'une intelligence artificielle reprend les principaux éléments de la définition de l'Organisation de coopération et de développement économiques (OCDE). Les logiciels libres seront exclus du champ d'application du règlement, à moins qu'il ne s'agisse de systèmes à haut risque, d'applications interdites ou d'IA dédiées à manipuler.

Gouvernance

- Un Bureau de l'IA sera créé au sein de la Commission afin de mettre en œuvre les dispositions concernant les modèles de fondation.

- Les systèmes d'IA seront supervisés par les autorités nationales compétentes, qui seront réunies au sein d'un **Comité européen de l'intelligence artificielle** afin de garantir une application cohérente de la législation à travers l'UE.

- Un forum consultatif recueillera les réactions des parties prenantes, y compris des acteurs de la société civile. Un groupe scientifique d'experts indépendants a également été mis en place pour donner des conseils sur l'application du règlement, signaler les risques systémiques et contribuer à la classification des modèles d'IA présentant des risques systémiques.

Les applications interdites	**Compte tenu de la menace potentielle pour les droits des citoyens et la démocratie, certaines applications de l'IA sont interdites** **- systèmes de catégorisation biométrique utilisant des caractéristiques sensibles (par exemple: opinions politiques, religieuses, philosophiques, orientation sexuelle, race));** **- extraction non ciblée d'images faciales sur Internet ou par vidéosurveillance pour créer des bases de données de reconnaissance faciale ;** **- reconnaissance des émotions sur le lieu de travail et les établissements d'enseignement;** **- la notation sociale basée sur le comportement social ou les caractéristiques personnelles ;** **- les systèmes d'IA qui manipulent le comportement humain pour contourner le libre arbitre ;** **- l'IA utilisée pour exploiter les vulnérabilités des personnes (en raison de leur âge, de leur handicap, de leur situation sociale ou économique).** **Les eurodéputés ont obtenu l'interdiction de la reconnaissance des émotions sur le lieu de travail et dans les établissements d'enseignement, avec une réserve pour des raisons de sécurité visant à reconnaître si, par exemple, un conducteur s'endort.** **Ils ont également introduit une interdiction des logiciels de police prédictive permettant d'évaluer le risque qu'une personne commette des crimes sur la base de ses caractéristiques personnelles.** **Le Parlement a insisté pour que les interdictions ne s'appliquent pas uniquement aux systèmes utilisés au sein de l'UE, mais qu'elles empêchent également les entreprises basées dans l'Union de vendre ces applications interdites à l'étranger.** **Toutefois, cette proposition n'a pas été maintenue car sa base juridique a été jugée insuffisante.**

Les applications à haut risque	Le règlement sur l'IA comprend une liste de cas d'utilisation considérés comme présentant un risque important d'atteinte à la sécurité et aux droits fondamentaux des individus. une série de conditions de filtrage destinées à ne retenir que les véritables applications à haut risque. Les domaines sensibles incluent : • l'éducation, • l'emploi, • les infrastructures critiques, • les services publics, • l'application de la loi, • le contrôle des frontières • l'administration de la justice. Le Parlement a réussi à introduire de nouveaux cas d'utilisation dans le cadre des utilisations à haut risque, comme les systèmes d'IA - prédisant les tendances migratoires et la surveillance des frontières. - influençant le résultat des élections et le comportement des électeurs
Obligations pour les systèmes à haut risque	Pour les systèmes d'IA classés comme présentant un risque élevé des obligations strictes ont été convenues, dont une analyse d'impact obligatoire sur les droits fondamentaux. Les citoyens auront le droit de déposer des plaintes concernant les systèmes d'IA et de recevoir des explications sur les décisions basées sur des systèmes d'IA à haut risque qui ont une incidence sur leurs droits.
Exemptions pour les services répressifs	Les fournisseurs et les organismes publics qui utilisent des systèmes d'IA à haut risque doivent les déclarer dans une base de données de l'UE. Les services de police et de contrôle des migrations disposeront d'une section spéciale non publique qui ne sera accessible qu'à une autorité de contrôle indépendante. Dans des circonstances exceptionnelles liées à la sécurité publique, les autorités répressives pourront utiliser un système à haut risque qui n'a pas passé la procédure d'évaluation de la conformité en demandant une autorisation judiciaire.

	Exceptions limitées pour l'utilisation des systèmes d'identification biométrique dans les espaces accessibles au public à des fins répressives, sous réserve d'une autorisation judiciaire préalable et pour des listes d'infractions strictement définies. **Les systèmes d'identification biométrique "à distance"** seront utilisés strictement dans le cadre de la recherche ciblée d'une personne condamnée ou soupçonnée d'avoir commis un crime grave. **Les systèmes d'identification biométrique "en temps réel"** répondront à des conditions strictes et leur utilisation sera limitée dans le temps et dans l'espace : - recherche ciblée de victimes (enlèvement, traite, exploitation sexuelle), - la prévention d'une menace terroriste précise et actuelle, ou - la localisation ou l'identification d'une personne soupçonnée d'avoir commis l'un des crimes spécifiques mentionnés dans le règlement (terrorisme, traite, exploitation sexuelle, meurtre, enlèvement, viol, vol à main armée, participation à une organisation criminelle, crime contre l'environnement).
Évaluation de l'impact sur les droits fondamentaux	Obligation pour les organismes publics et les entités privées fournissant des services publics essentiels, tels que les hôpitaux, les écoles, les banques et les compagnies d'assurance déployant des systèmes à haut risque, de procéder à une évaluation de l'impact de l'utilisation de l'IA sur les droits fondamentaux.
Systèmes généraux d'Intelligence Artificielle - Modèles de fondation	Enjeu **L'absence de régulation d**es modèles de fondation développés par les **géants** comme Microsoft ou Google **impactera** les industries qui les utilisent pour développer et fournir des applications spécifiq**ues.** **Les industriels utilisateurs seront les seul**s responsables de toute fiabilité défaillante du modèle. **Cette option rendrait** ces industries vulnérables et dépendantes des fournisseurs de modèles de fondation**.** **Rejet de la mise en place de règles contraignantes** **La France, l'Allemagne et l'Italie** ont **fait** pression pour que les règles qui concernent les modèles de fondation au sein du règlement européen relatif à l'intelligence artificielle se limitent à des codes de conduite, sans sanctions, plutôt que d'imposer des obligations normatives

les systèmes d'IA à usage général, et les modèles sur lesquels ils sont basés, devront respecter
-des exigences de transparence, comme initialement proposé par le Parlement.
Il s'agit notamment :

- de mettre à jour la documentation technique,
- de se conformer à la législation de l'UE sur les droits d'auteurs
- de diffuser des résumés détaillés sur le contenu utilisé pour leur formation.

Des obligations de transparence s'appliqueront à tous les modèles, notamment la publication d'un résumé suffisamment détaillé des données d'entraînement « sans préjudice des secrets commerciaux » de l'entreprise développeuse de l'IA.

Les contenus générés par des IA devront également être directement reconnaissables.

Modèles avancés présentant un risque systémique
Les modèles avancés seront soumis à des obligations plus strictes telles que **:**
- l'évaluation de modèle ;
- évaluer et atténuer les risques systémiques,
- effectuer des tests contradictoires ;
- rendre compte à la Commission des incidents graves,
- assurer la cybersécurité,
- rendre compte de leur efficacité énergétique

Les codes de conduite seront uniquement destinés à compléter les obligations jusqu'à ce que des normes techniques harmo**nisées soient mises en place,**
la Commission pourra intervenir par le biais d'actes délégués si le processus prend trop de temps.

Modèle open source
L'AI Act ne s'appliquera pas aux modèles open source et gratuits dont les paramètres sont rendus publics, à l'exception des aspects relatifs au respect des droits d'auteur, à la publication d'un résumé détaillé, aux obligations pour les modèles systémiques et aux responsabilités tout au long de la chaîne de valeur de l'IA.

Mesures de soutien à l'innovation et aux PME : Bac à sable réglementaire	L'accord promeut des "bacs à sable réglementaires", et des environnements réels, mis en place par les autorités nationales pour développer et tester une IA innovante avant sa mise sur le marché.
Responsabilité au sein de la chaîne d'approvisionnement	Les fournisseurs de systèmes d'IA à usage général comme ChatGPT devront fournir toutes les informations nécessaires pour se conformer aux obligations de l'AI Act aux fournisseurs économiques situés en aval dans la chaîne d'approvisionnement qui créent une application qualifiée à haut risque.
Amendes	Les amendes administratives sont fixées à un montant minimum ou à un pourcentage du chiffre d'affaires annuel global de l'entreprise, si ce dernier est plus élevé. Le non-respect des règles peut entraîner des amendes allant de 7,5 millions d'euros ou 1,5 % du chiffre d'affaires à 35 millions d'euros ou 7 % du chiffre d'affaires mondial, en fonction de l'infraction et de la taille de l'entreprise.

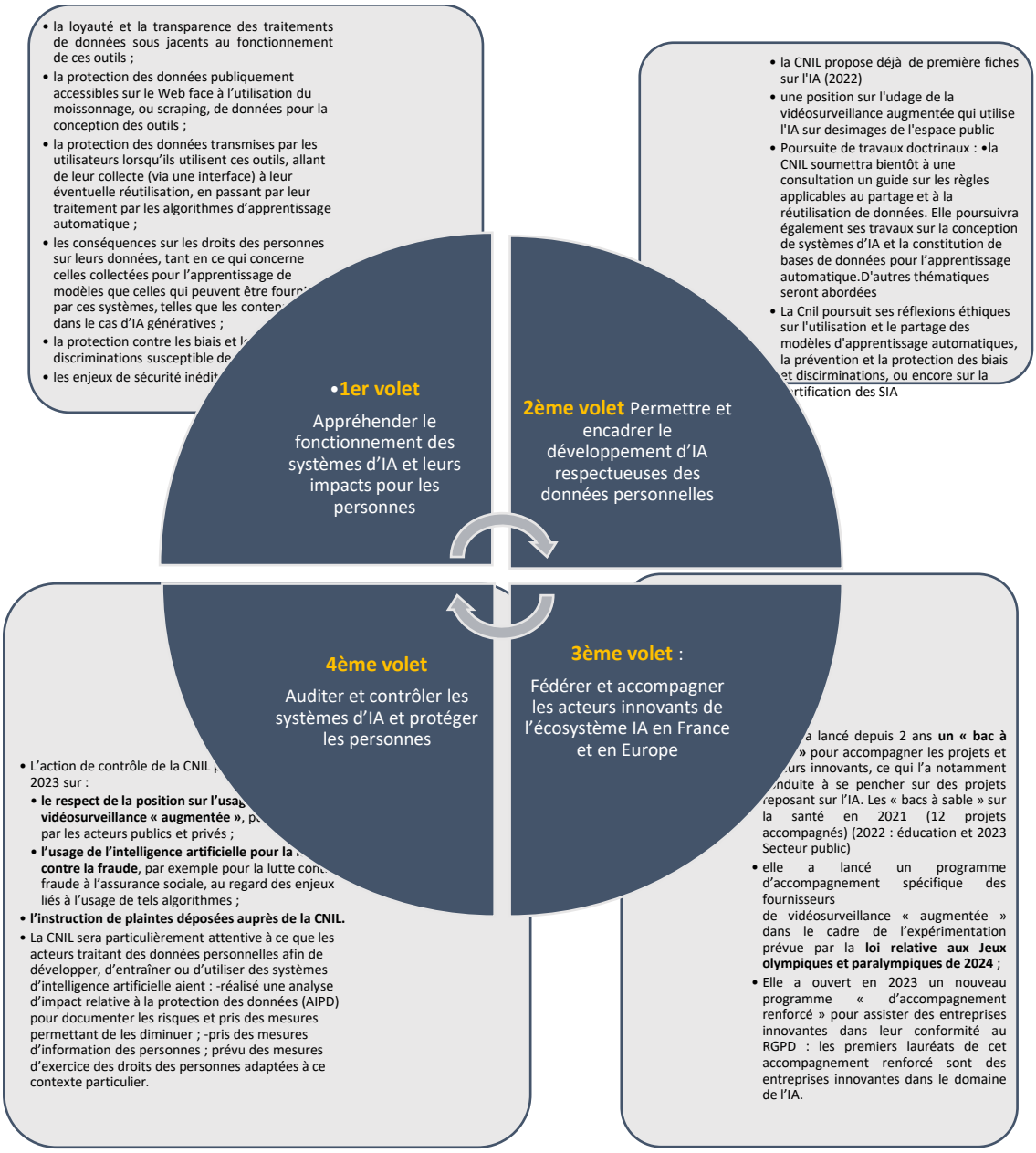
Le règlement sur l'IA s'appliquera deux ans après son entrée en vigueur, le délai étant écourté à six mois pour les interdictions.

Les exigences relatives aux systèmes d'IA à haut risque, aux modèles d'IA puissants, aux organismes d'évaluation de la conformité et au chapitre sur la gouvernance commenceront à s'appliquer au bout d'un an.

Focus sur l'IA et la CNIL

Au niveau national, la CNIL travaille depuis plusieurs années sur le sujet de l'intelligence artificielle qui constitue une nouvelle génération d'algorithmes ou, au sens de loi Informatique et Libertés, de traitements de données. La CNIL s'est également prononcée sur des projets à propos desquels le gouvernement a requis son avis.

Le plan d'action sur l'IA de la CNIL



Conformité du système d'IA avec le RGPD

Cas particulier des systèmes d'IA

La mise en place d'un système d'IA reposant sur l'apprentissage automatique nécessite la succession de deux phases :

finalité relative à la phase d'apprentissage :

La phase d'apprentissage consiste à concevoir, développer et entraîner un système d'IA et en particulier un modèle, c'est-à-dire une représentation de ce que le système d'IA aura appris à partir des données d'entraînement.

Finalité relative à la phase de production :

La phase de production consiste à déployer de manière opérationnelle le système d'IA obtenu à l'étape 1.

Du point de vue de la protection des données, **ces deux étapes ne remplissent pas le même objectif et doivent donc être séparées.** Dans les deux cas la finalité des traitements de données personnelle effectués lors de chacune de ces phases devra être déterminée, légitime et explicite.

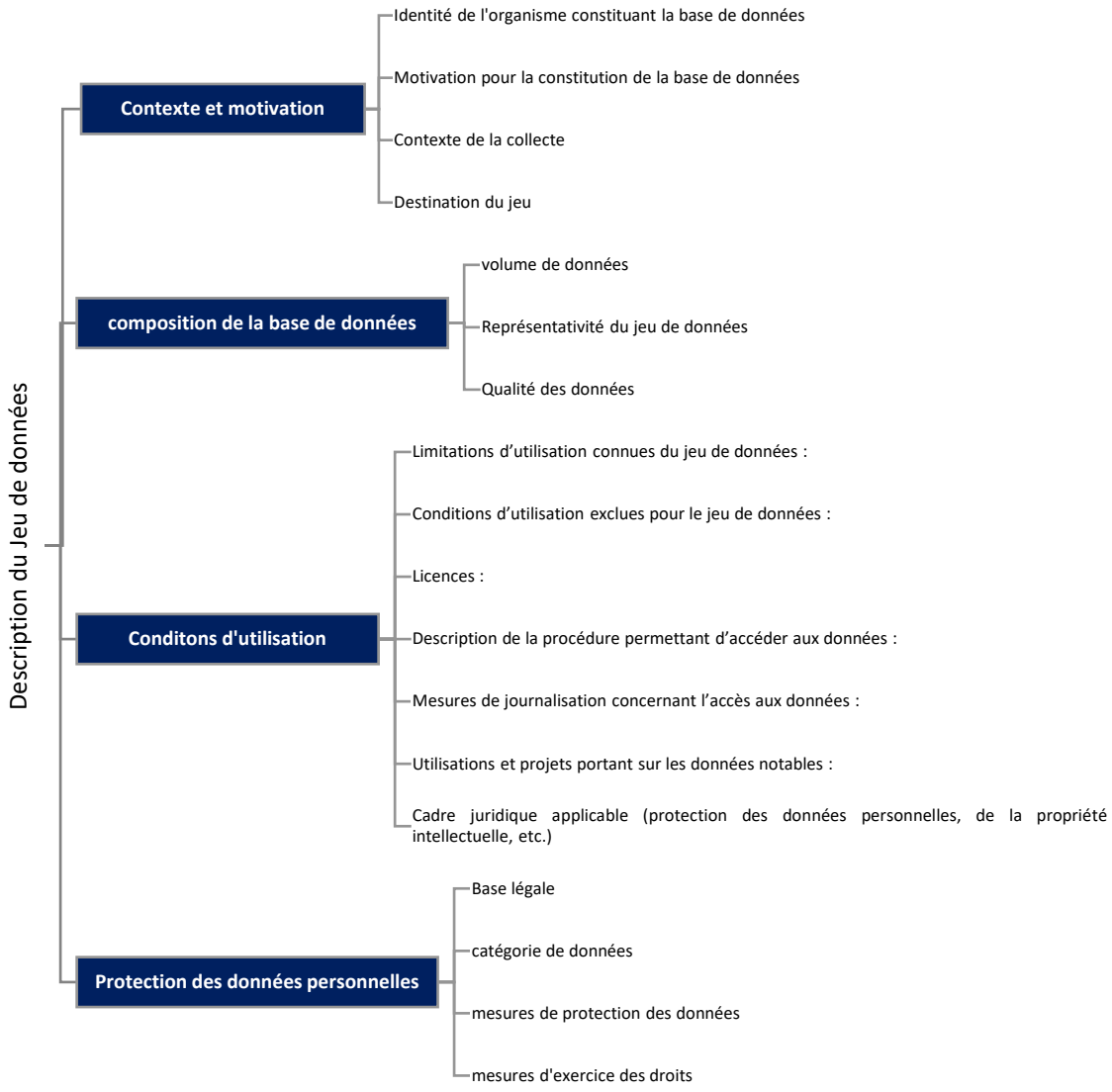
Se prémunir des risques liés aux modèles d'IA (représentations de ce que l'IA a appris à partir des données d'apprentissage)	Taxonomie des attaques des systèmes d'IA : principaux risques • Attaques par inférence d'appartenance, • Attaque par exfiltration de modèle • Attaque par inversion de modèle Un modèle d'IA entrainé à partir de données personnelles ne peut, par défaut, être considéré lui-même comme une donnée personnelle (ou plus exactement un ensemble de données personnelles). Cependant, sa constitution doit se fonder sur une exploitation licite des données au sens du RGPD. si un modèle d'IA fait l'objet d'une attaque en confidentialité réussie, cela peut constituer une violation de données. Il est alors nécessaire de procéder au retrait du modèle en question dans les plus brefs délais et de procéder à une notification de violation de données auprès de l'autorité de protection des données compétente si la violation est susceptible d'entraîner un risque pour les droits et libertés des personnes concernées.
S'assurer de l'information et de l'explicabilité	Le principe de transparence du RGPD exige que toute information ou communication relative au traitement de données personnelles soit concise, transparente, compréhensible et aisément accessible, en des termes simples et clairs. l'information à donner aux personnes peut varier : • lorsque les données n'ont pas été collectées directement par le responsable mettant en œuvre le système d'IA et qu'il est difficile de revenir vers les personnes concernées (dérogation au droit à l'information);

	• pour l'exercice de certains droits (notamment de l'article 22 du RGPD), il est indispensable de fournir des explications précises à la personne concernée sur les raisons ayant conduit à la prise de décision en question.
Encadrer la prise de décision automatisée	Le responsable du traitement doit donc prévoir la possibilité, d'une intervention humaine de sa part pour permettre à la personne concernée d'obtenir un réexamen de sa situation, d'exprimer son point de vue, d'obtenir une explication sur la décision prise et de contester la décision. En cas d'aide à la décision, des garanties sont aussi nécessaires, notamment en termes d'information.
Évaluer le système	L'évaluation des systèmes d'IA est un enjeu essentiel et au cœur du projet de règlement de la Commission européenne. Du point de vue de la protection des données, celle-ci est indispensable pour : • Valider l'approche testée lors de la phase de conception et de développement du système (dite « phase d'apprentissage ») (fonctionne conformément aux attentes des concepteure). • Minimiser les risques de dérive du système qui peuvent être observés au cours du temps. • S'assurer que le système, une fois déployé en production, satisfait bien les besoins opérationnels pour lesquels il a été conçu. Il faut en effet dissocier les performances obtenues lors de la phase d'apprentissage de celle du système une fois placé en phase de production, la qualité des premières ne préjugeant pas de celle des secondes.
Éviter les discriminations algorithmiques	L'utilisation de systèmes d'IA peut également entrainer des risques de discriminations. Les raisons sont multiples et peuvent provenir : • des données utilisées pour l'apprentissage ; • de l'algorithme lui-même qui présenterait des failles de conception.

En santé, le recours au système d'intelligence artificielle s'impose pour développer une médecine personnalisée de prévention.
L'entraînement des algorithmes consomme un volume important de données, notamment de données personnelles, soumises au RGPD. L'usage des algorithmes et des systèmes d'intelligence artificielle basés sur l'entrainement automatique de *type machine learning* sont utilisés dans la phase de détection et d'aide au diagnostic. Leur fonctionnement repose sur le traitement des données, très souvent personnelles. Le respect des exigences du RGPD impose notamment une l'information des personnes concernées et des utilisateurs par le responsable de traitement, ce qui nécessite une compréhension du fonctionnement du Système d'IA.

Description du jeu de données

La CNIL a élaboré une fiche descriptive du jeu de données comprenant les items suivants :



REX « Bac à sable » de la CNIL : Santé Numérique

Le « bac à sable » données personnelles de la CNIL est un dispositif d'accompagnement à destination des innovateurs d'un secteur sur des problématiques émergentes. Ce dispositif s'inscrit dans l'action de la CNIL en soutien à l'innovation. Le « bac à sable » fonctionne sur une logique de co-construction entre le porteur de projets et les équipes de la CNIL. Le « bac à sable » s'adresse donc aux organismes confrontés à des problématiques nouvelles en lien avec la réglementation données personnelles. En intervenant à un stade précoce de développement du projet, les équipes de la CNIL aident l'organisme à identifier les solutions possibles, et à les implémenter.

Les étapes du « bac à sable » de la CNIL :

Un accompagnement « bac à sable » se déroule sur plusieurs mois et comprend trois séquences :

- **Phase d'accompagnement (6 mois)** : Identification des problématiques à traiter, constitution de la feuille de route de l'accompagnement
- **Phase d'implémentation** : déploiement des recommandations de la Cnil
- **Phase de retour à l'écosystème** : publication des recommandations de la Cnil sur les différents systèmes

La CNIL publie les recommandations formulées aux différents porteurs de projet lors de son accompagnement « bac à sable », pour en faire bénéficier les acteurs du secteur de la santé numérique et aider les innovateurs sur des projets similaires à développer leur solution. En santé numérique, les recommandations ont été publiées en février 2022. Elles reflètent l'état de la réglementation à cette date.

Projets ayant bénéficié du bac à sable en Santé Numérique

L'apprentissage fédéré entre plusieurs entrepôts de données de santé	**CHU de Lille et Inria**
Une solution d'aide au diagnostic en oncologie	Résilience

Des indicateurs statistiques anonymes de description des populations en recherche médicale	Clinityx
Un jeu thérapeutique pour les mineurs atteints de troubles alimentaires	Centre hospitalier d'Arras

Projet de l'apprentissage fédéré entre entrepôts de données de santé

Le projet du CHU de Lille et de l'équipe Magnet de l'Inria : mettre en œuvre un procédé d'apprentissage fédéré entre plusieurs entrepôts de données de santé

De juin à décembre 2021, la CNIL a accompagné le CHU de Lille, en coopération avec d'autres centres hospitaliers de la région, sur la mise en place d'un protocole d'apprentissage fédéré portant sur un algorithme visant à faciliter la prise en charge des patients et utilisant des données hébergées dans plusieurs entrepôts de données de santé (EDS). La technique de l'apprentissage fédéré, qui permet de développer un modèle d'intelligence artificielle sans centraliser les données, a soulevé plusieurs questions auxquelles la CNIL a répondu lors de son accompagnement.

L'apprentissage fédéré pour entraîner une IA : technique de protection de la vie privée ?

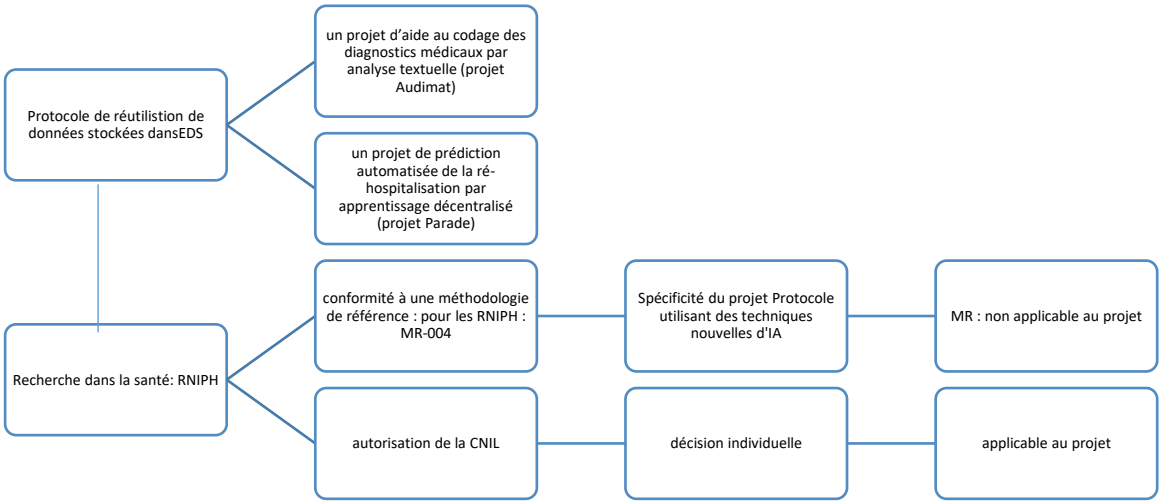
3 Questions à la CNIL (procédure de bac à sable)

Question 1 : Nature des agrégats ?
Question n°2 : Cadre juridique des exports ?
Question n°3 : Sécurisation du traitement

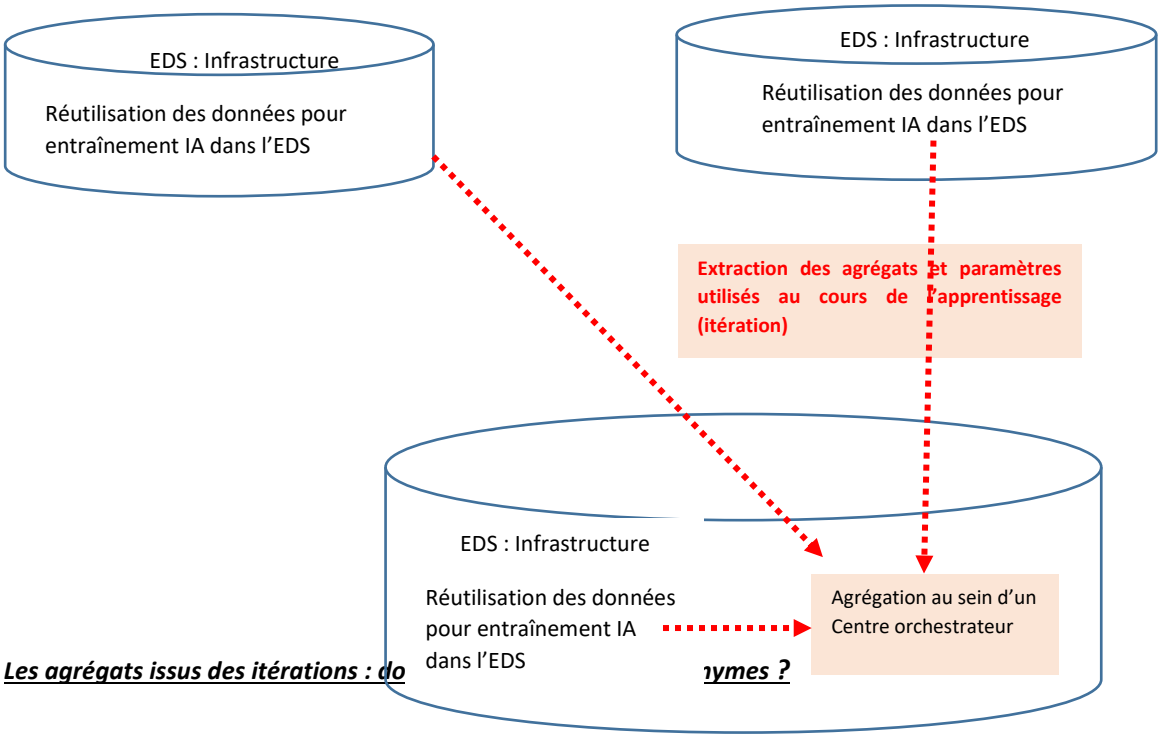
Réutilisation des données des EDS dans le cadre d'une RNIPH

S'agissant du contexte juridique, les données des entrepôts de données de santé (EDS) concernés, autorisés par la CNIL, ont pu **être réutilisées dans le cadre d'une recherche n'impliquant** pas la personne humaine (RNIPH), sous réserve du respect de certaines exigences réglementaires.

Le protocole, en ce qu'il utilise des techniques innovantes d'intelligence artificielle, a été considéré comme un projet de recherche dans le domaine de la santé, et sa réalisation est donc soumise au respect des formalités applicables.



Volet Technique : Apprentissage fédéré



Les agrégats issus des itérations : do ıymes ?

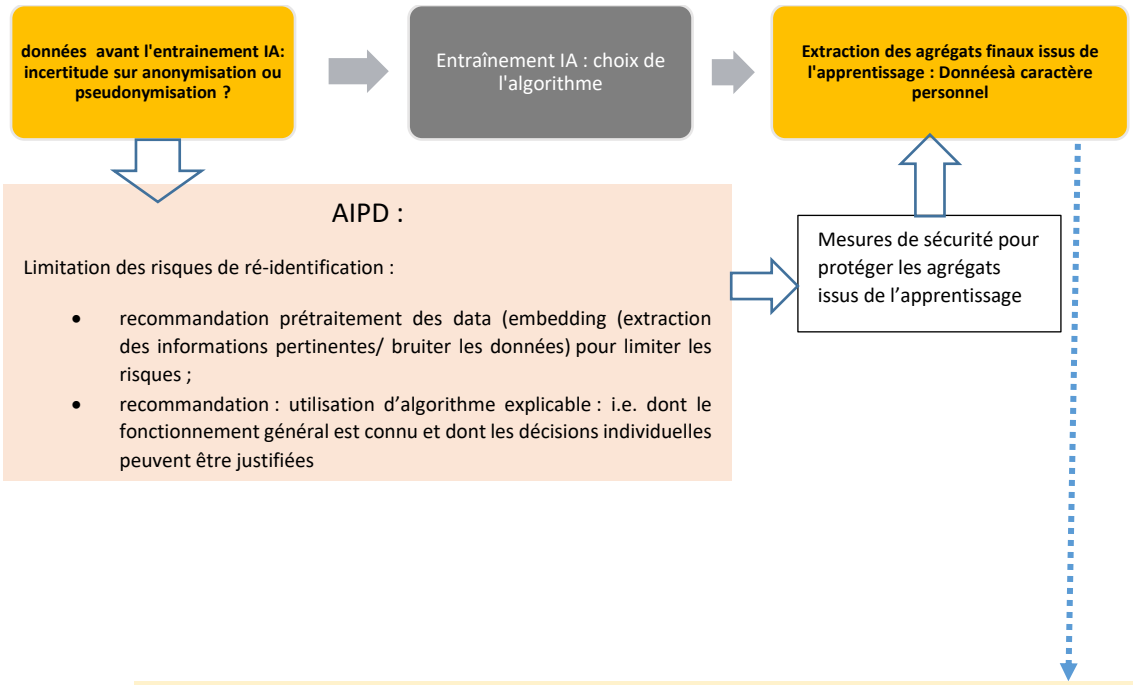
Afin d'apprécier cette nature, le responsable de traitement (RT) a été encouragé à vérifier le caractère anonyme des données le plus en amont possible dans le traitement envisagé, un résultat issu de l'agrégation de données anonymes pouvant être considéré comme anonyme à son tour.

Option n°1 : données anonymisées avant l'apprentissage IA

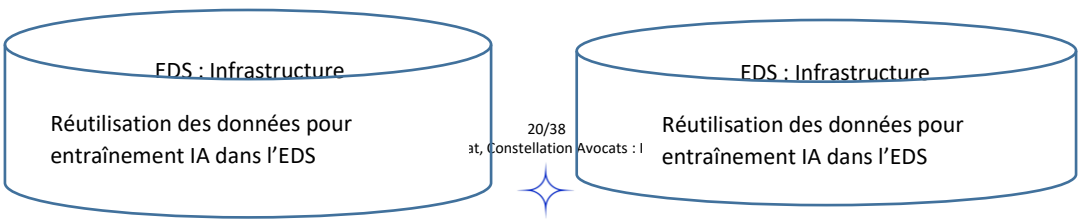
- Données anonymisées avant l'entrainement IA
- Entraînement IA : Extraction des agrégats finaux issus de l'apprentissage : Données Anonymisées

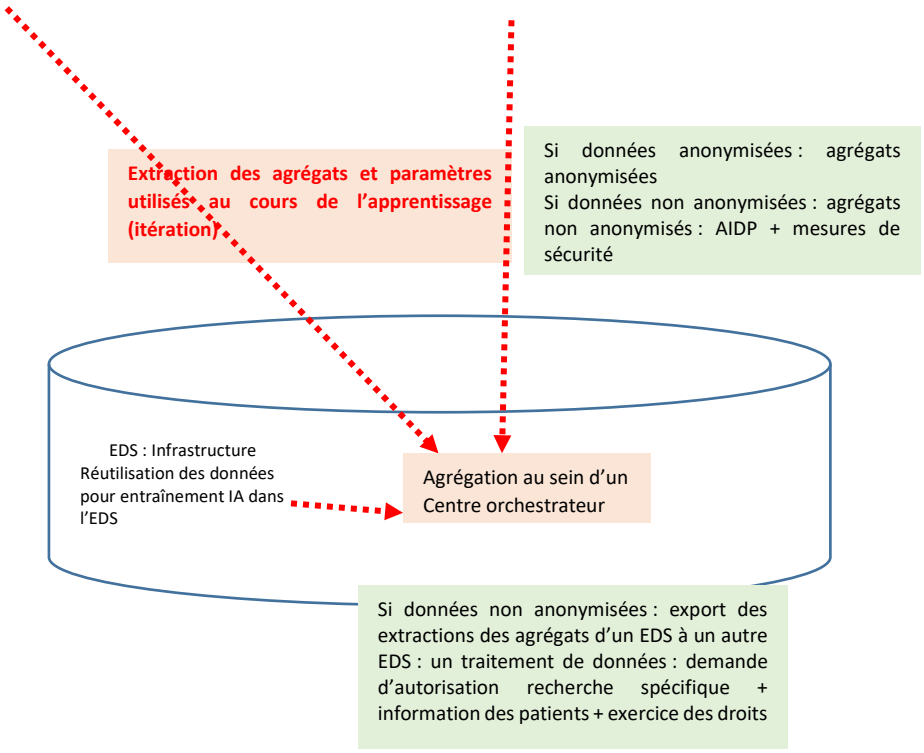
Option n°2 : Incertitude sur les données dans la base d'entraînement

- Lorsque le caractère anonyme des données d'entraînement ne peut être vérifié, une analyse des risques de réidentification portant sur les agrégats finaux ou utilisés au cours de l'apprentissage doit être réalisée.



Cadre juridique de l'export de données non anonymes d'un EDS
Si données non anonymisées : export (extraction des agrégats) est un traitement de données : demande d'autorisation recherche spécifique + information des patients + exercice des droits :
Chiffrement TLS des communications, mesures de sécurité propre à l'apprentissage fédéré : chiffrement homorphe (une méthode permettant de réaliser des opérations sans perte de confidentialité des données chiffrées)





Le projet de Resilience : une solution d'aide au diagnostic en oncologie

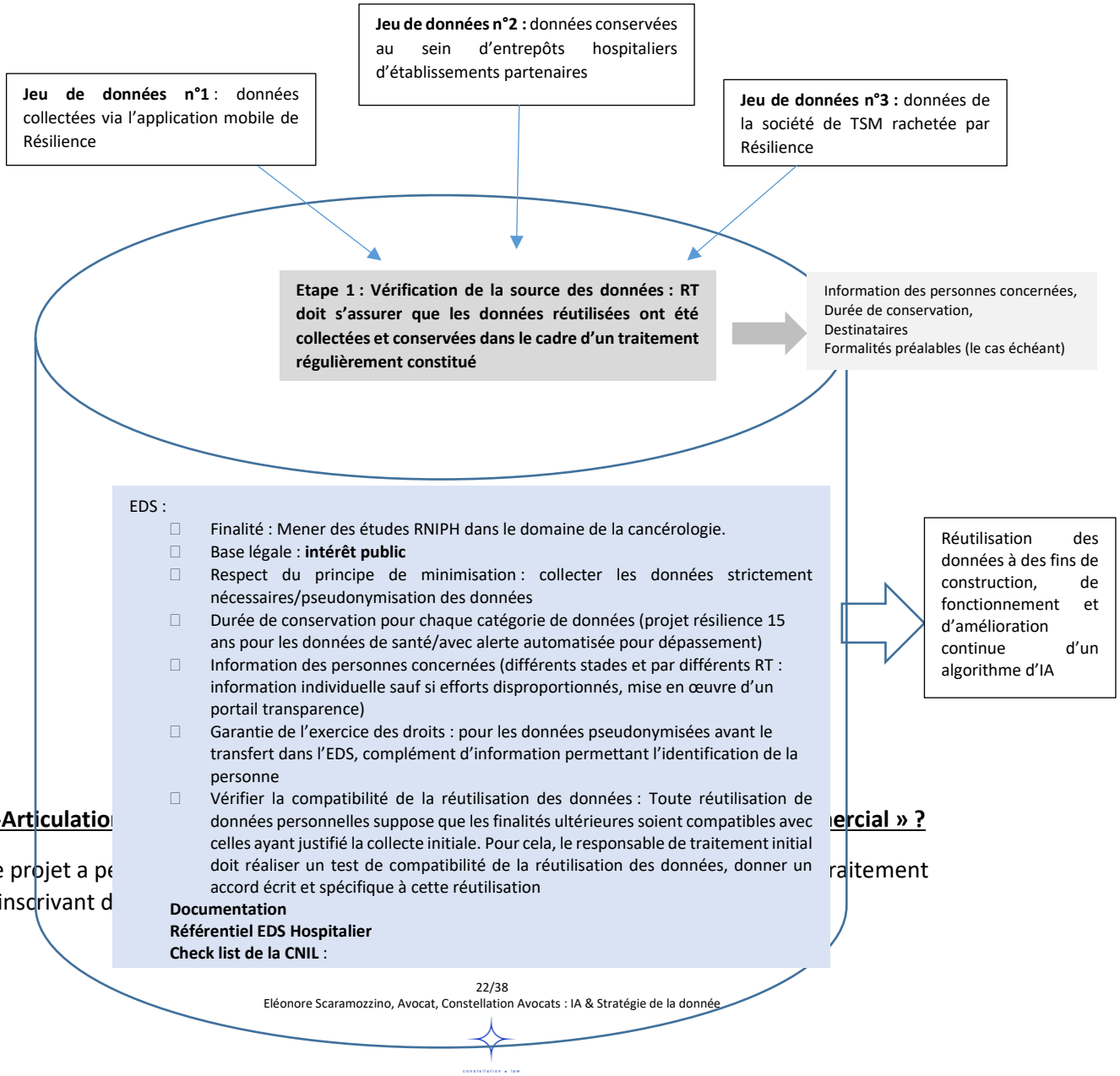
En 2021, la CNIL a accompagné Resilience souhaitant proposer une application mobile d'éducation thérapeutique et un logiciel d'aide à la prise de décision médicale fonctionnant grâce à un algorithme d'intelligence artificielle. Pour réunir ces deux outils, Resilience a souhaité créer un entrepôt de données de santé notamment alimenté par des données collectées via son application mobile et des données conservées au sein d'entrepôts hospitaliers d'établissements partenaires. Au cours de son accompagnement, la jeune pousse a racheté une société de télésurveillance : les données issues de ce type de suivi ont donc été ajoutées aux deux premiers jeux de données.

3 Questions à la CNIL (procédure bac à sable »)

1. **Comment rassembler les données de différentes sources pour constituer un entrepôt ?**
2. **Comment articuler le concept d'intérêt public avec un traitement s'inscrivant dans un cadre commercial ?**
3. **Quelle démarche pour utiliser les données d'un entrepôt à des fins de construction, de fonctionnement et d'amélioration continue d'un algorithme d'intelligence artificielle ?**

1 Rassembler les différents jeux de données dans un EDS

Ces échanges avec la CNIL ont permis d'organiser l'interconnexion de différentes sources ainsi que la réutilisation des données rassemblées.



2-Articulatio ercial » ?

Le projet a pe raitement s'inscrivant d

La base légale d'un traitement sur « ***l'exécution d'une mission d'intérêt public*** ». est uniquement mobilisable par les personnes morales de droit public ou les personnes morales de droit privé investies d'une mission de service public.

Position de la CNIL

Tous les traitements de données personnelles dans le domaine de la santé comportent, par définition, des données de santé. La législation9 prévoit que ces traitements doivent « ***être mis en œuvre en considération de la finalité d'intérêt public qu'ils présentent*** ».

Les critères permettant d'établir cette finalité d'intérêt public tiennent :

- aux objectifs et bénéfices du traitement mis en œuvre ;
- aux modalités d'organisation envisagées (dans le cadre d'un entrepôt par exemple : l'objectif du traitement, les modalités de transparence, l'intégrité scientifique, la qualité des études, etc.).

Par principe, cette finalité d'intérêt public des traitements en santé n'est pas incompatible avec les intérêts – notamment commerciaux – d'une personne morale relevant du secteur privé.

La CNIL a souligné que :

« la condition de « finalité d'intérêt public » ne correspond pas à la base légale du traitement (art. 6 du RGPD) mais à l'exigence prévue par les articles 44-3° et 66 de la loi « informatique et libertés » modifiée.

Dans sa décision autorisant le projet d'entrepôt de données de santé RESILIENCE, la CNIL a estimé que le traitement poursuit une finalité d'intérêt public.

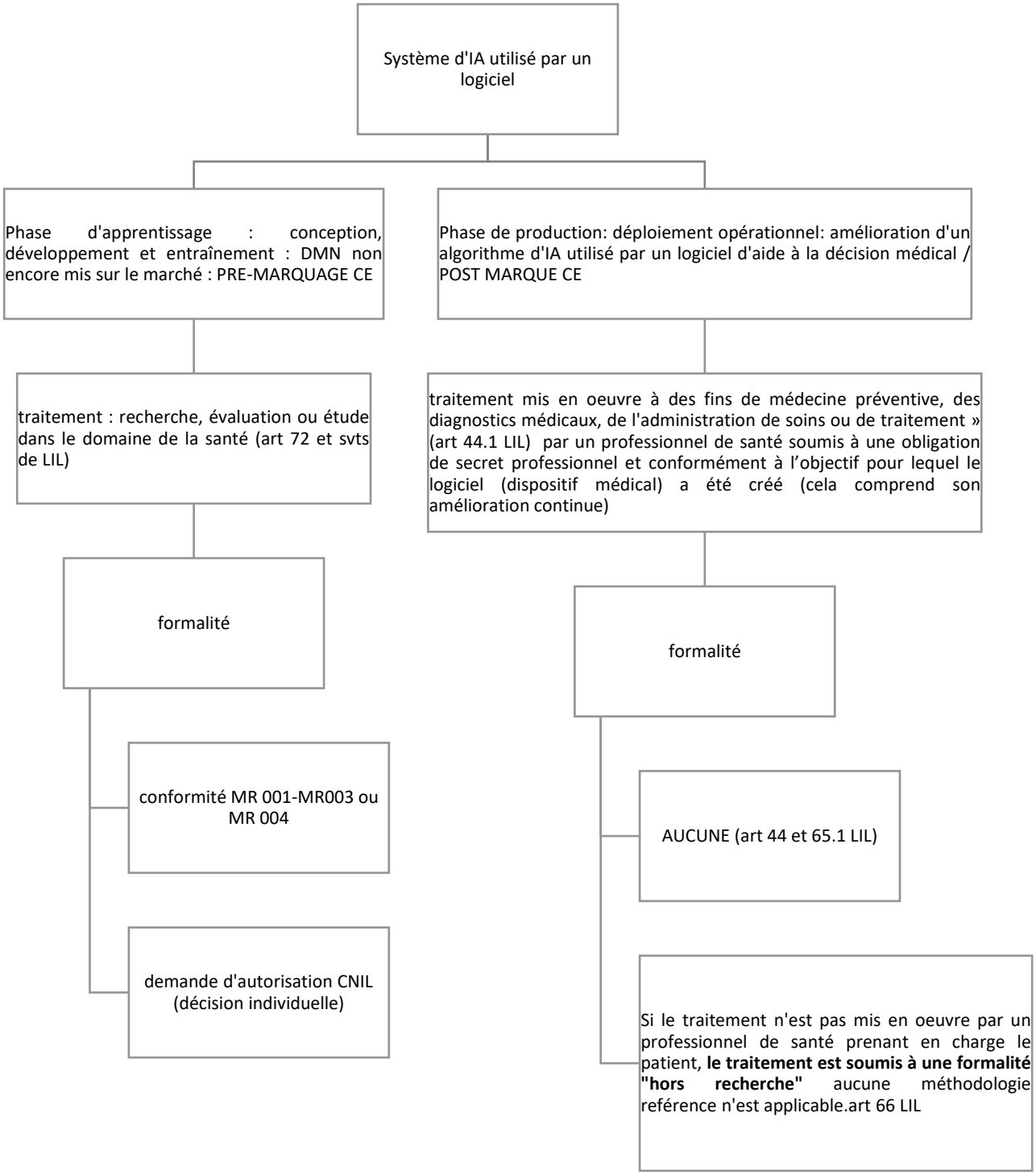
Délibération n°2022-049 du 21 avril 2022 autorisant RESILIENCE SAS à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données dans le domaine de la santé, dénommé « Resilience Data Warehouse » (Demande d'autorisation n° 2224863)

Sur la base légale du traitement
Le traitement envisagé a pour base légale l'intérêt légitime, au sens de l'article 6-1-f du RGPD.

Le traitement de données sensibles est nécessaire aux fins de recherche scientifique (art. 9.2.j du RGPD) et de garantie des normes élevées de qualité et de sécurité des dispositifs médicaux, sous réserve qu'il soit fondé sur une disposition nationale ou européenne (art. 9-2-i du RGPD).

3. Réutilisation des données d'un entrepôt à des fins de construction, de fonctionnement et d'amélioration continue d'un algorithme d'intelligence artificielle

Dans le projet de Resilience, la CNIl va apporter des précisions sur les conditions à satisfaire pour réutiliser les données de santé aux fins de développement, d'amélioration continue et de fonctionnement d'algorithmes d'IA.
Formalités, en fonction des étapes de vie de l'algorithme et de la qualité du responsable de traitement.



Le traitement mis en oeuvre à des fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitement » (art 44.1 LIL) par un professionnel de santé soumis à

une obligation de secret professionnel et conformément à l'objectif pour lequel le logiciel (dispositif médical) a été créé (cela comprend son amélioration continue)

2 conditions :

- le logiciel est utilisé par un professionnel de santé prenant en charge la personne, responsable de traitement et soumis au secret professionnel.

- le logiciel est utilisé « **en vie courante** » à des fins de médecine préventive, de diagnostic, d'administration de soins ou de traitements.
  Pour déterminer si le logiciel intégrant un algorithme d'IA est utilisé **« en vie courante** », plusieurs critères peuvent être pris en compte :
  - utilisation par des professionnels de santé dans leur activité quotidienne,
  - impact direct potentiel pour le patient,
  - apprentissage intrinsèque de l'algorithme au fil de l'eau,
  - utilisation du logiciel conforme aux spécifications de son marquage CE, etc.

Focus sur le DATA GOVERNANCE ACT (DGA)

Pour créer son marché unique des données, la Commission européenne a établi un cadre harmonisé pour l'échange des données personnelles et non personnelles. Ces nouvelles règles sont précisées dans le règlement européen sur la gouvernance des données DATA GOVERNANCE ACT (DGA), adopté en mai 2022 et entré en vigueur le 24 septembre 2023. Il vise à exploiter le potentiel de données générées par les entreprises, le secteur public, les citoyens, en créant un cadre harmonisé des pratiques au sein de l'UE, favorisant le partage de données personnelles et non personnelles via des structures d'intermédiation, qui pourront prendre la forme de plateformes numériques permettant le libre partage ou contrôle de leurs données par les entreprises et particuliers.

Conditions de réutilisation de certaines données protégées du secteur public

Le DGA organise la réutilisation de "certaines données protégées" détenues par des organismes du secteur public.

Ces données sont :

- des données protégées pour des motifs de confidentialité commerciale ;
- des données relevant de secret statistique ;
- des données protégées par des droits de propriété intellectuelle ;
- des données à caractère personnel protégés par le RGPD.

Conditions de la réutilisation des données des organismes du secteur public,

Les organismes du secteur publics compétents pour octroyer ou refuser l'accès aux données, doivent rendre publiques la procédure et les conditions d'autorisation de cette réutilisation.

- Ces conditions doivent être "**non discriminatoires, transparentes, proportionnées et objectivement justifiées**".
- **Conservation du caractère protégé des données**. Les données doivent être anonymisées. Ainsi, la technique d'anonymisation utilisée doit rendre impossible et ce de manière irréversible toute identification de la personne physique. L'accès et la réutilisation des données doivent se faire dans "un environnement de traitement sécurisé dans le respect des normes de sécurité élevées".
- **Interdiction des accords d'exclusivité**. Seule exception : lorsque le droit d'exclusivité est nécessaire à "la fourniture d'un service ou d'un produit d'intérêt général" qui, sans cela, ne pourrait être obtenue. La durée de cette exclusivité ne doit alors pas dépasser 12 mois.
- **Redevance pour la réutilisation des données**. Elles devront être "transparentes, non discriminatoires, proportionnées" et ne devront pas restreindre la concurrence.

Services d'intermédiation de données reconnus dans l'UE

Le principal apport du DGA est la création **des services d'intermédiation de données,** qui vont permettre de partager des données. Ces structures peuvent prendre par exemple la forme de plateformes numériques.

- **Procédure de notification à l'autorité nationale chargée des données** : La fourniture de ce service est soumise à une procédure de notification à l'autorité compétente (Commission nationale de l'informatique et des libertés (Cnil) en France). Cette notification doit contenir : le nom du prestataire, son statut juridique, son adresse, son contact, la description du service et sa date de lancement.

- **Label** : après autorisation par l'autorité compétente, le service peut utiliser le label "**prestataire de services d'intermédiation de données reconnu dans l'Union**" dans ses communications écrites et orales ainsi qu'un logo commun.

- **Réutilisation dans une Finalité déterminée** : Les services d'intermédiation de données ne peuvent pas utiliser les données à des fins autres que celles initialement prévues.

- **Tarification non liée à l'utilisation d'autres services** : les modalités commerciales ne peuvent pas être liées à l'utilisation de leurs autres services par le détenteur de données.

- **Format des données** : les données collectées dans des formats spécifiques ne peuvent être converties dans d'autres formats uniquement "pour améliorer l'interopérabilité intersectorielle et transsectorielle" ou si l'utilisateur le demande.

Data altruism

Le DGA prévoit également **des règles en matière de** *data altruism*, une façon d'inciter les parties prenantes à partager les données qu'elles estiment utiles pour l'intérêt général. Il oblige la désignation d'une autorité compétente pour l'enregistrement des organisations altruistes. Elle devra tenir un registre public national des organisations reconnues dans ce domaine.

Une fois enregistrées, ces dernières disposeront d'un logo commun, établi par la Commission européenne, accompagné d'un QR code comportant un lien vers le registre public.

Un comité européen de l'innovation dans le domaine des données

Comité européen de l'innovation dans le domaine des données
Mission Conseil de la Commission européenne

Ce groupe d'experts sera composé de

- représentants des autorités compétentes en matière de services d'intermédiation de données ;
- des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de tous les États membres,
- du comité européen de la protection des données,
- du Contrôleur européen de la protection des données,
- de l'Agence de l'Union européenne pour la cybersécurité (ENISA),
- de la Commission européenne,
- du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME,
- d'autres représentants d'organismes compétents dans des secteurs particuliers ;
- d'organismes disposant d'une expertise particulière.

Autorité nationale
chaque Etat membre doit nommer une autorité chargée de superviser au niveau national l'application du DGA

Dans un avis publié en mai 2022, le Comité européen de la protection des données (CEPD), le Contrôleur européen de la protection des données (EDPS) et la Cnil française avaient alerté sur le fait que la non-désignation par le texte d'une autorité spécifique pouvait entraîner une réelle complexité pour les parties prenantes et nuire à la cohérence de la surveillance de l'application du RGPD. Etant que rien ne s'oppose à ce qu'elle fasse les deux, l'autorité française pourra être l'autorité chargée de superviser l'application du DGA.

Focus sur le DATA ACT

Le Data Act vise à définir un cadre pour faciliter l'accès et l'utilisation des données personnelles et non personnelles.

Il prévoit :

- d**e faciliter le partage entre entreprises (B2B) et avec le consommateur (B2C)** des données, en fixant une obligation de rendre accessibles les données générées par l'utilisation "*des objets connectés et services connexes*" en contrepartie d'une compensation juste et équitable.
- **des clauses contractuelles types** visant à protéger les PME contre les clauses contractuelles abusives imposées par une partie disposant d'un pouvoir de négociation nettement supérieur et à aider ces PME à rédiger et à négocier des contrats de partage équitable des données ;
- **de conférer aux organismes du secteur public des moyens pour accéder aux donnée**s et utiliser les données détenues par le secteur privé qui sont nécessaires pour faire face à des circonstances exceptionnelles, notamment en cas d'urgence publique (inondation, incendie de forêt, par exemple), ou pour exécuter un mandat juridique si les données ne sont pas rendues disponibles par un autre moyen ;
- **d'élaborer des normes d'interopérabilité** pour le partage des données et les services de traitement des données, conformément à la stratégie de normalisation de l'UE ;
- **de mettre en place des garanties contre les accès illicites de gouvernements de pays tiers** aux données non-personnelles contenues dans le cloud ;
- **de faciliter le passage entre différents fournisseurs de services cloud**, favorisant la concurrence et le choix sur le marché.
- **de réviser le règlement sur la base de données :** Le règlement sur les données révise en outre certains aspects de la directive sur les bases de données, qui avait été adoptée dans les années 1990 pour protéger les investissements dans la présentation structurée de données. Ainsi, il sera possible d'avoir accès aux bases de données contenant des données provenant de dispositifs et d'objets de l'internet des objets et de les utiliser.
- **de permettre aux consommateurs et entreprises d'accéder aux données de leur appareil** et les utiliser pour le service après-vente et des services à valeur ajoutée tels que la maintenance prédictive.

Articulation DATA ACT ET DGA avec le RGPD

Les autorités et le CEPD reconnaissent que ces textes poursuivent des objectifs légitimes. Néanmoins, elles alertent sur l'importance d'une bonne articulation avec le RGPD. "*La protection des données personnelles est*

essentielle et fait partie intégrante de la confiance dans le développement de l'économie numérique", rappelle la Cnil. Cette recommandation a été prise en compte puisque qu'il a été prévu qu'en cas de conflit, le RGPD prévaudra sur le DGA.

Les autorités nationales de protection des données en Europe et le Contrôleur exigent "*des garanties additionnelles*" concernant les droits d'accès, d'utilisation et de partage des données prévues par le Data Act. De plus, des précisions doivent être apportées sur les notions "*d'urgence publique*" et de "*besoin exceptionnel*" lorsqu'il y a une obligation de mise à disposition des données aux organismes du secteur public et institutions de l'UE.

La question de l'autorité de supervision du DATA ACT et du DGA

Ni le DGA, ni le DATA ACT ne désigne les autorités chargées de la supervision de l'application des textes. Les autorités nationales chargées de l'application du RGPD recommandent donc au législateur européen de désigner les autorités de protection des données comme autorités coordinatrices. En effet, les autorités de protection des données ont "*une expertise juridique et technique dans la supervision des traitements de données personnelles, et l'accompagnement des acteurs et modèles d'affaires innovants*".

Focus sur règlement sur l'espace européen commun des données de santé : EHDS

European Health Data Space

Le 3 mai 2022, la Commission européenne a publié une proposition de règlement portant création d'un espace européen des données de santé (EHDS European Health Data Space), considérée comme un pilier essentiel de l'union européenne de la santé. Cette proposition est le premier de neuf espaces européen de données spécifiques à certains secteurs et domaines définis par la Commission dans sa communication de 2020 intitulée "Une stratégie européenne pour les données".

Cette proposition poursuit trois objectifs: garantir l'utilisation primaire des données de santé; établir des règles relatives aux solutions proposées sur le marché en ce qui concerne les systèmes de dossiers médicaux et les applications de bien-être; et autoriser l'utilisation secondaire des données de santé sous certaines conditions. Elle définit également les règles, les infrastructures et le cadre de gouvernance nécessaires au développement de l'utilisation primaire (y compris transfrontière) et secondaire des données de santé.

Objectif

L'objectif de l'EHDS est de faciliter l'accès aux données de santé et l'échange de ces dernières entre les Etats membres de l'UE afin de :

- **donner la main aux européens** sur leurs données de santé électronique ;
- **soutenir la fourniture des soins de santé lors des déplacements au sein de l'UE** ("utilisation primaire des données") ;
- **améliorer le fonctionnement du marché unique** pour la mise au point et de l'utilisation de produits et services de santé ;
- **Faciliter la réutilisation des données de santé électronique** par les chercheurs, les innovateurs et les décideurs politiques pour l'élaboration des politiques dans le domaine de la santé (réutilisation des données, également appelée "utilisation secondaire des données") ;

Utilisation primaire et secondaire des données

La proposition prévoit :

Utilisation primaire,

- droit d'accéder gratuitement à leurs données de santé à caractère personnel dans un format électronique.
- Certaines de ces données figurent sur une liste de six catégories prioritaires, notamment les dossiers de patients et les images médicales.
- L'interopérabilité au sein de l'Union devrait être assurée.

Utilisation secondaire

- soumise à autorisation de l'organisme responsable de l'accès

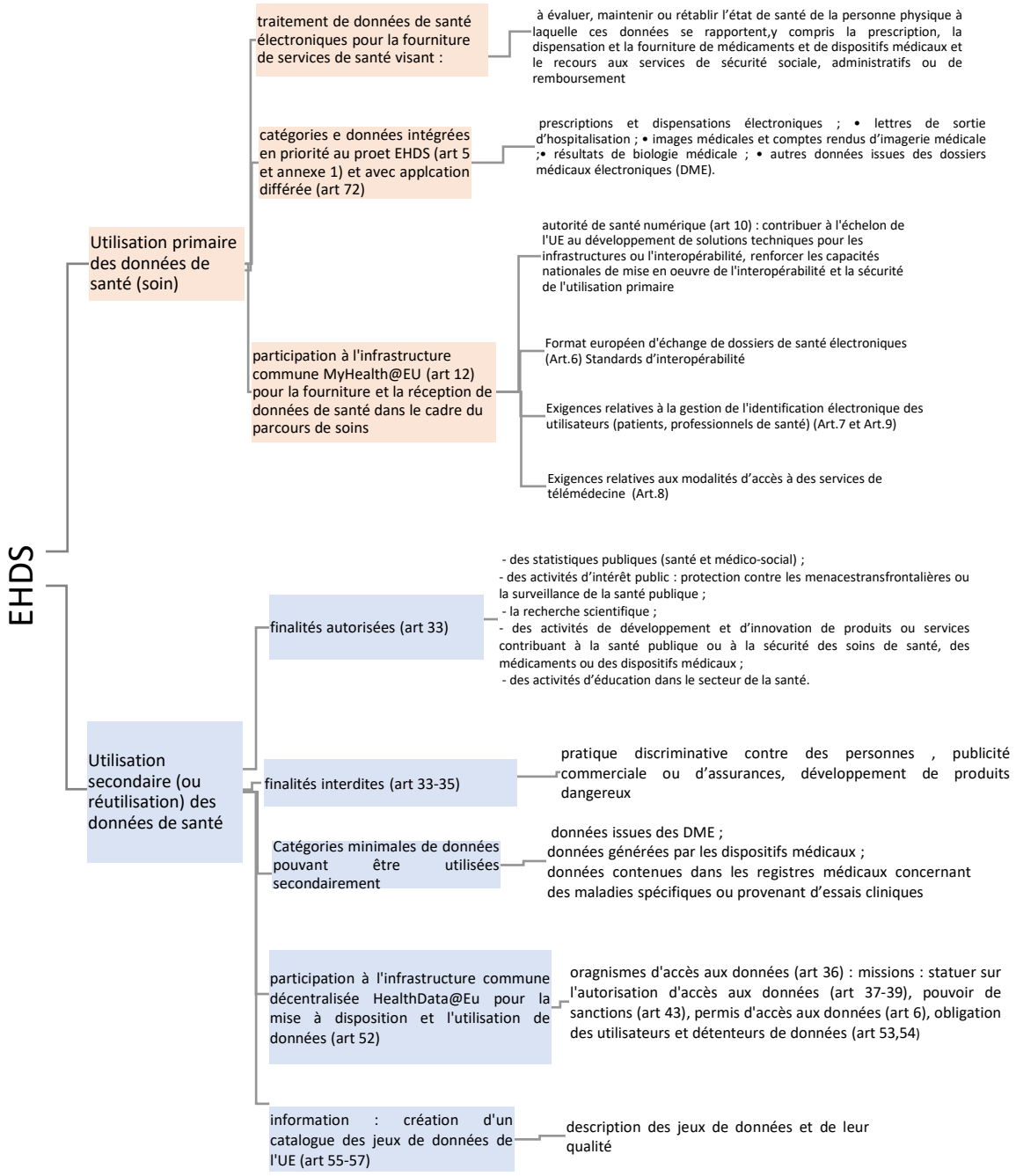
aux données de santé dans chaque État membre.

- Huit catégories de finalités licites sont prévues à cet effet, telles que la recherche scientifique, l'intérêt public ou l'innovation, y compris la création de systèmes d'intelligence artificielle.
- Les cas où la réutilisation des données de santé est interdite sont répartis en six catégories.

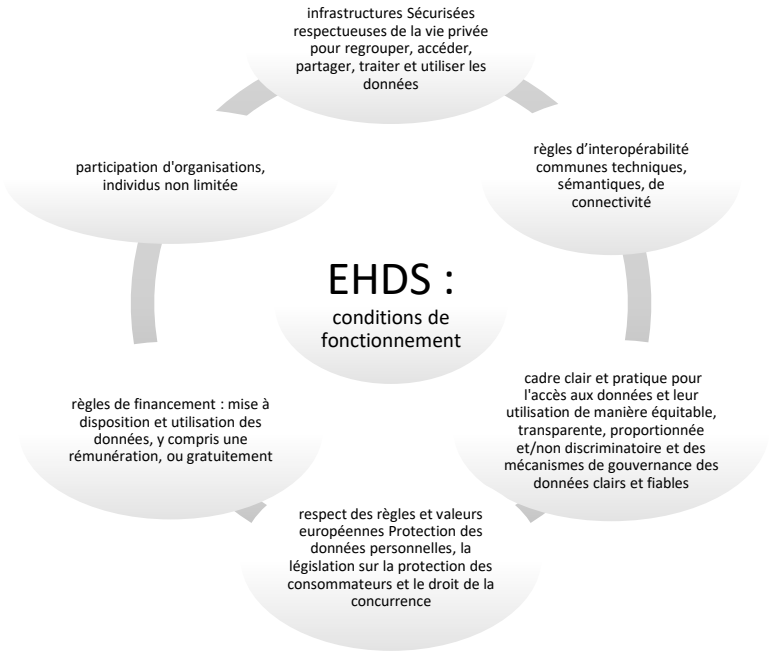
Mécanisme d'autocertification

La proposition prévoit un mécanisme d'autocertification obligatoire pour les systèmes de dossiers médicaux électroniques (DME), qui devraient être conformes aux spécifications communes que la Commission adoptera.

Synthèse



Conditions de fonctionnement de l'EHDS



Les infrastructures de l'EHDS

MyHealth@EU: utilisation primaire des données de santé

Infrastructure existante

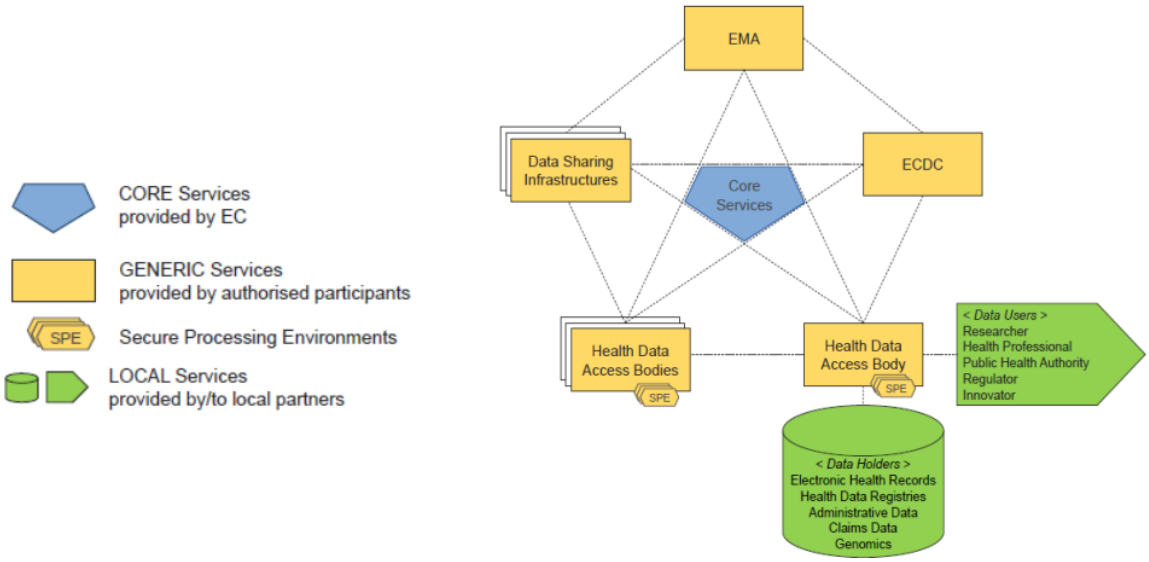
- 11 Etats membres connectés dont la France
- 2 services opérationnels
  - e-prescrption
  - patient summary

HealthData@EU : utilisation secondaire (réutilisation) des données de santé

Infrastructure inexistante à créer au niveau européen pour faciliter l'accès transfrontière aux données de santé. Au niveau national, des organismes responsables de l'accès aux données de santé examineront les demandes d'accès aux données et délivreront des autorisations de traitement de données.

Le Health Data Hub coordonne un consortium de 16 partenaires pour créer un pilote de HealthData@EU

Infrastructure à créer



Lancement du projet pilote :

HEALTH Data Hub est à la tête d'un consortium fédérant 16 entités partenaires –EHDS 2 Pilot Consortium

Objectifs du projet pilote

- Développer et déployer un réseau de services socles (core services) et plateformes (nœuds) permettant de connecter les pays participants via leurs points de contrôle nationaux (health data access bodies) mais aussi certains organismes européens tels que l'ECDC ou l'EMA ;

- Evaluer la faisabilité et la capacité des Etats à déployer une telle infrastructure à l'échelle de l'UE

Négociations interinstitutionnelles

Position du Parlement européen

Le 13 décembre 2023, le Parlement européen a adopté par 516 voix pour, 95 contre et 20 abstentions, des amendements à la proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé. La question a été renvoyée aux commissions compétentes pour négociations interinstitutionnelles.

Position du Conseil

Le 6 décembre 2023, les États membres de l'UE ont approuvé le mandat de négociation avec le Parlement européen du Conseil concernant le règlement relatif à un espace européen des données de santé (EHDS).

La présidence du Conseil de l'UE dispose à présent d'un mandat pour entamer les négociations avec le Parlement européen dès que possible, en vue de parvenir à un accord provisoire sur la proposition de règlement

A suivre …en 2024

constellation • law

Collectif d'avocats et de médiateurs

Pour toute information complémentaire ou question vous pouvez contacter directement l'auteur

Eléonore Scaramozzino
Avocat
Constellation Avocats
escaramozzino@constellation.law

constellation • law