Qu'est-ce que la donnée numérique de santé et comment la protéger ?

Intervention Christian Viallon Ressourcial Journée NEC Grand Est 9 avril 2024

A l'intitulé de cet atelier peut-être conviendrait-il d'ajouter « *pourquoi* » et/ou « *contre qui* » ou « *contre quelles menaces* » ?

Mais il faut d'abord, se poser la question : qu'est-ce qu'une donnée de santé ?

La notion de donnée de santé : une notion très large

- Parce que le concept de santé est lui-même très large. Si l'on retient la définition de l'OMS (Organisation mondiale de la Santé) : « *La santé est un état de complet bien-être physique, mental et social et ne consiste pas seulement en une absence de maladie ou d'infirmité* »[1].
- Parce que l'origine des données de santé est diverse, on peut distinguer schématiquement :
  - Celles qui sont des données de santé par **nature** : maladies, antécédents médicaux, prestations de soins, handicaps…
  - Les données qui, **croisées avec d'autres**, communiquent des informations sur l'état de santé ex : mesure du poids croisée avec apports caloriques,
  - Celles qui sont des données de santé par **destination**. Par exemple : mesure du poids dans analyses biologiques.

Pour aujourd'hui je vous propose de retenir la définition que donne le Règlement général sur la protection des données (RGPD) dans son considérant 35 : Définition : « **Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne** ».

Principales sources de données numériques de santé

Les sources sont multiples, on peut en citer quelques-unes, de façon non exhaustive :

- Les bases de données médico-administratives : Par exemple, le Sniiram (Système national d'information inter-régimes de l'Assurance maladie) contient 8,9 milliards de feuilles de soins. Ces bases de données enregistrent des informations sur les prestations de soins réalisées.
- Les images d'actes d'imagerie : Chaque année, environ 80 millions d'actes d'imagerie (comme les radiographies, IRM, etc.) génèrent des données de santé.
- Les cohortes et registres : Ces ressources rassemblent des informations sur des groupes de patients pour des études de recherche ou de suivi.
- Les dossiers médicaux : Les dossiers médicaux des patients, tenus par les professionnels de santé, contiennent des données de santé importantes.
- Les essais cliniques : Les essais cliniques recueillent des données sur l'efficacité et la sécurité des traitements.
- Les données collectées via les smartphones, les réseaux sociaux et les sites internet : De plus en plus, les patients partagent des informations sur leur santé via ces canaux.

[1] https://www.who.int/fr/about/frequently-asked-questions

- Les données qui résultent d'opérations de réidentification : Renseignement d'Origine Source Ouverte (ROSO ou OSINT).

Quel est l'intérêt du traitement numérique des données de santé ?

À titre individuel le traitement numérique permet de

- documenter le parcours de soin
- renseigner le dossier personnel : Mon espace santé
- offrir au patient l'opportunité de jouer un rôle plus actif dans la prise en charge de sa maladie en lui donnant les informations
- fournir des informations précises sur l'état de santé d'un individu à qui a à en connaître : professionnel de santé, notamment.

Ce traitement doit contribuer à atteindre l'objectif affirmé dans les politiques publiques (très récemment encore dans la loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé – dite Ma santé 2022) : *vivre vieux et en bonne santé*.

À titre collectif le traitement numérique revêt notamment un intérêt en

- épidémiologie
- garantie de la qualité des soins
- prévention des risques sanitaire ex : polluants éternels et eau de consommation
- prévention en santé .

En raison du périmètre très large qu'elles couvrent mais aussi en raison de l'intérêt qu'elles revêtent au plan individuel comme au plan collectif les données de santé doivent être protégées. Le secret médical pour ne prendre que cet aspect particulier s'impose depuis des millénaires et passe dès le XIXème siècle dans le domaine juridique.

Les données de santé à caractère personnel sont protégées … jusqu'à un certain point

Loi Informatique et libertés - 6 janvier 1978

Aux origines on trouve la conjonction de notions telles que le secret médical (qui remonte au serment d'Hippocrate) et la protection de la vie privée. La formalisation de cette protection s'agissant en particulier du traitement informatique des données s'inscrit formellement dans le droit français à partir du 6 janvier 1978 avec la *Loi Informatique et libertés*. Rappeler la genèse de cette loi n'est pas sans intérêt par rapport au sujet qui nous rassemble cette après-midi. La loi Informatique et libertés découle d'un mouvement qui est né en 1974 autour du projet SAFARI. Le journal Le Monde dans son édition du 21 mars 1974[2] titre « *Une division de l'informatique est créée à la chancellerie " Safari " ou la chasse aux Français* ». L'acronyme SAFARI, si bien nommé, désignait le Système automatisé pour les fichiers administratifs et le répertoire des individus.

La France et l'Allemagne sont précurseurs dans ce domaine. Rapidement on prend conscience que le sujet de la protection des données à caractère personnel dépasse le cadre national. Dans le cadre européen on commence par adopter des directives (non contraignantes) pour arriver en 2016 au RGPD.

---

[2] [en ligne] https://www.lemonde.fr/pixels/article/2024/03/21/il-y-a-cinquante-ans-un-article-du-monde-declenchait-la-creation-de-la-cnil_6223203_4408996.html consulté le 25/3/2024

Règlement Général sur la Protection des Données (RGPD)

Règlement européen (dans la hiérarchie des normes un règlement s'impose aux états membres de l'Union européenne à la différence d'une directive qui doit être transposée dans le droit national) adopté le 27 avril 2016 et entré en vigueur le 25 mai 2018.

Sous l'empire du RGPD les données de santé sont particulièrement protégées (elles sont communément appelées « *données sensibles* »). L'Art 9 du RGPD interdit leur traitement SAUF si

- le consentement au traitement est donné par la personne,
- des obligations particulières qui s'imposent au responsable de traitement,
- l'utilisation est encadrée par le droit du travail,
- le traitement est opéré dans le cadre de la sécurité sociale,
- le traitement est opéré dans le cadre de la protection sociale,
- des motifs d'intérêt public nécessitent le traitement : ex : COVID,
- la sauvegarde des intérêts vitaux de la personne est en jeu,
- le traitement s'inscrit dans des travaux de recherche (cette éventualité est très encadrée par des Méthodologies de référence établies par la CNIL).

La réglementation ainsi que des initiatives françaises et européennes (récentes) renforcent la sécurité vis-à-vis notamment des cyberattaques :

- Programme CaRE (lancé en décembre 2023) [3]:
  - éviter que les attaques aboutissent,
  - permettre aux établissements de s'en relever le plus rapidement possible
- Transposition de la directive NIS2 dans la réglementation française [4]

Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information) : la directive NIS 2 s'appuie sur les acquis de la directive NIS 1 pour marquer un changement de paradigme, tant à l'échelon national qu'à l'échelon européen. Face à des acteurs malveillants toujours plus performants et mieux outillés, touchant de plus en plus d'entités trop souvent mal protégées, la directive NIS 2 élargit en effet ses objectifs et son périmètre d'application pour apporter davantage de protection. Cette extension du périmètre prévue par NIS 2 est sans précédent en matière de réglementation cyber.

Les Français souhaitent que leurs données de santé soient protégées

86% des Français considèrent leurs données de santé comme particulièrement sensibles et redoutent, pour 78% d'entre eux, qu'elles soient utilisées à des fins commerciales ou qu'elles fassent l'objet de piratage. (Source Ministère travail santé et solidarités février 2024 Le numérique en santé : ce qu'en pensent les Français - Ministère du travail, de la santé et des solidarités).

En ce sens les Français ont raison : ils perçoivent, plus ou moins confusément, les enjeux autour de leurs données de santé quitte à avoir vis-à-vis de celles-ci une attitude paradoxale.

---

[3] [en ligne] https://esante.gouv.fr/strategie-nationale/cybersecurite#:~:text=Le programme CaRE prend en,num%C3%A9rique et de la cybers%C3%A9curit%C3%A9. Consulté le 25/3/2024

[4] [en ligne] https://cyber.gouv.fr/la-directive-nis-2 consulté le 25/3/2024

Les données de santé à caractère personnel : entre enjeux de santé publique, enjeux commerciaux et cible du grand banditisme

La donnée de santé comme moteur de la recherche médicale

Aujourd'hui les technologies de l'information permettent de conjuguer l'augmentation de la puissance de calcul des ordinateurs avec les possibilités offertes par l'intelligence artificielle. Afin, par exemple, de :

- fouiller de grandes masses de données,
- établir des corrélations,
- détecter des maladies invisibles à l'œil nu pour faire de la
    - médecine prédictive,
    - médecine de précision,
    - médecine préventive,
- aider à la décision,
- aider à évaluer la gravité d'une pathologie (ex : tri en services d'urgence),
- suivre des patients à distance (télémédecine, téléconsultation),
- conduire des actes de chirurgie assistée par ordinateur,
- mettre en place des robots compagnons. ex : Oreille Augmentée des Soignants (système d'alerte nocturne qui se base sur l'analyse du contexte sonore et permet, grâce à l'intelligence artificielle, d'alerter les soignants sur différents risques captés par le son), mais aussi bien d'autres dispositifs : ex : pilulier connecté, mais aussi robotique,
- utiliser les données issues du "*quantified self*" (mesure de soi) :
    - analyser son activité physique ou son mode de vie : poids, tension, calories consommées, nombre de pas dans la journée, rythme cardiaque, etc.
    - bracelets, podomètres, montres ou applications mobiles connectées aux capteurs d'un smartphone, etc.
- interpréter de grandes masses de données, les étudier et rendre compte en langage naturel.

Les données de santé deviennent la matière première de l'industrie du médicament

Les "big pharma" et la stratégie "beyond the pill"

Les big pharma ce sont 5 grands groupes et environ 50 multinationales de l'industrie du médicament. Leur analyse aujourd'hui les conduit à conclure que leurs sources de profit se trouve *au-delà du médicament* (beyond the pill). Elles entendent déployer une approche "holistique" :

- en s'appuyant sur les applis mobiles,
- en proposant des offres de coaching,
- en démontrant l'efficacité du médicament (auprès de l'assurance maladie par exemple).

La stratégie « *beyond the pill* » est déclinée par la big pharma selon 5 P, soit une approche :

- Personnalisée : spécifique à chaque patient,
- Prédictive : capacité d'évaluer la probabilité d'une personne de développer une maladie,
- Préventive : aider à prévenir les maladies,
- Participative : mettre le patient au centre en mettant à sa disposition des outils pour prendre soin de sa santé
- Populationnelle : une offre disponible pour le plus large public.

On conçoit bien que la stratégie "*beyond the pill*" suppose la capacité à collecter et traiter des masses de données toujours plus grandes. A ce point les intérêts des Big pharma et des GAFAM se rejoignent !

Les GAFAM[5] et autres géants du net

Aux origines la fortune des GAFAM (Google, Apple, Facebook, Amazon, et Microsof) et autres géants du net s'est établie sur le ciblage publicitaire profilé des internautes, elles ont très vite compris l'intérêt du réemploi de l'information via des plateformes multifaces. C'est ce mécanisme que Shoshana Zuboff[6] décrit comme le *capitalisme de surveillance*[7]. Depuis au moins 10 ans elles ont décidé d'investir la esanté. La esanté, selon la définition de l'OMS[8] c'est le regroupement des services numériques qui sont au service du bien-être des personnes. Cette définition englobe aussi l'utilisation des outils de production, de partage et de gestion des informations numérisées en vue d'optimiser les pratiques médicales et médico-sociales. La esanté c'est un marché estimé à 234 milliards de $.

Google (Alphabet)

Investit le marché de la esanté depuis 2009. En 2020 relance Google health. Domaine d'activité particulier les wearables : objets informatiques et électronique, destinés à être portés sur soi. Vêtements ou accessoires connectés à un appareil (ex : téléphone,) pour recueillir des données relatives à la personne qui les porte et à son environnement.

Microsoft azure cloud

Héberge le health data hub français.

En 2018 lancement de Microsoft genomic, 2019 lancement de Azure health bot : robot conversationnel pour l'accompagnement administratif du patient.

Amazon

2023 : rachat de One Medica entreprise qui propose des soins de santé primaires en ligne. Développe une offre de service en santé mentale (Mindset). 2018 lancement de l'assurance médicale Haven.

En France Amazon héberge les données de Doctolib sur AWS. Amazon est aussi partenaire de IQVIA qui, par exemple) collecte et revente de données de santé des pharmacies françaises (cf. Cash investigation 20/05/2021).

Apple

Déclaration de Tim Cook PDG d'Apple « la plus grande contribution d'Apple à l'humanité concerne le domaine de la santé ». On peut citer les applis Health et le healthkit. Aux USA l'applewatch est classée comme dispositif médical. Apple a pour perspective la vente de services d'analyse et d'influence comportementale (le nudge).

Meta Facebook

2023 le NHS britannique partage sur Facebook les données de santé de ses patients. L'hôpital pour enfants Alder Hay Children's Hospital de Liverpool a également transmis à Facebook et Méta des renseignements sur les prescriptions de médicaments.

---

[5] Cette partie est documentée à partir de l'ouvrage Le business de nos données médicales – Enquête sur un scandale d'Etat (2021) de Boulard A, Favier-Baron E, Woillet S. Editions FYP

[6] Zuboff S.(2020) L'âge du capitalisme de surveillance. Editions Zulma. Paris

[7] Selon Zuboff le capitalisme de surveillance est un nouvel ordre économique qui revendique l'expérience humaine comme matière première gratuite à des fins de pratiques commerciales dissimulées d'extraction, de prédiction et de vente.

[8] [en ligne] https://www.who.int/europe/fr/news/item/09-09-2020-digital-health-transforming-and-extending-the-delivery-of-health-services consulté le 12 avril 2024

Meta a des liens avec Palantir[9]. Palantir est une entreprise de services et d'édition logicielle spécialisée dans l'analyse et la science des données (communément appelé « Big data »), basée à Denver dans le Colorado. Palantir a remporté un contrat de 330 millions de livres pour créer une nouvelle plateforme de données destinée au British National Health Service (NHS).

Outre ces quelques exemples il faut aussi évoquer l'osmose entre GAFAM et administration publique qui s'exprime de façon toute particulière dans le « *pantouflage* ».

Le pantouflage un sport national dans la haute administration française et européenne

- plus de 250 anciens employés de la Commission européenne travaillent pour Amazon (130), Google (89), Microsoft (55), Facebook (51) ou Apple (23)

Quelques cas personnels :

Benoit Lourcel, 2013-2016 : DG de l'ARCEP (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse), 2017 : directeur des relations institutionnelles et des politiques publiques de Google France.

Alexandre Quintard fondateur d'Etalab (modernisation de l'action publique française), 2015 : chargé des affaires publiques et des relations gouvernementales d'Uber France.

Laurent Solly, sous-préfet, directeur de campagne de Nicolas Sarkozy. Président de Facebook France

Jean-Marc Aubert, directeur de la DREES (direction de la recherche et de l'évaluation statistique, chargé du lancement du Health data hub. 2019 : Président de IQVIA France

Quels risques la situation que l'on vient de décrire fait-elle courir à nos données de santé ?

- La perte de souveraineté sur nos données de santé.
- Les effets probables de la privatisation de domaines régaliens (ex : le Health data hub français chez Microsoft).
- Evidemment l'objectif des GAFAM et des autres géants du net est le profit et non l'intérêt général.
- L'hyper concentration dans d'énormes entrepôts de données les rend beaucoup plus sensibles aux attaques que ne le seraient leur répartition dans des systèmes distribués sous contrôle citoyen.

La grande criminalité

Il ne se passe guère de semaine sans que les médias ne fassent état d'attaques dont est victime tel ou tel service hospitalier. Selon le CERT Santé (ANS) Service d'appui à la gestion des cybermenaces, en 2023[10] :

- 467 structures de santé ont déclaré un incident
  - 71% établissements de santé
  - 22% des ESSMS
- 581 incidents
  - Dont 60% ont eu un impact sur les données

[9] Palantir a été mêlé au scandale Facebook/Cambridge Analytica qui a éclaté en 2018

[10] Selon la Quotidien du médecin (13/3/2024) https://www.lequotidiendumedecin.fr/hopital/securite-des-soins/cybersecurite-le-fleau-422-etablissements-de-sante-ont-declare-au-moins-un-incident-en-2023

On estime qu'un dossier médical se négocie jusqu'à 250€ sur le darknet quand une carte bancaire se négocie à 5€.

Les services hospitaliers cibles privilégiées des attaques. Les assaillants ne sont pas des geeks mangeurs de pizza déployant leurs attaques depuis le huis clos de leur studio. On est en présence d'une "*industrie*" ayant pignon sur rue dans certains pays où ils bénéficient d'une garantie d'impunité totale quand il ne s'agit pas de l'incitation des pouvoirs publics. Nous sommes en présence d'un dispositif organisé avec planning, système de congés, autorisation d'absence, etc. pour assurer la gestion des « *employés* ». On peut évoquer :

- Russie : Killnet
- Chine
- Soudan : Anonymus sudan

Qui sont les clients ? Il faut considérer que la "*clientèle*" n'est pas que criminelle (pour susciter par exemple des arnaques diverses et variées). Dans cette clientèle on peut imaginer trouver : les compagnies d'assurance, les Etats, Vincent Trély, président de l'APSSIS (Association pour la sécurité des systèmes d'information de santé) a détaillé ces hypothèses dans le Quotidien du médecin[11] (aout 2022). Il prend l'exemple des données de recherche : imaginez que l'on dérobe à un hôpital cinq années de recherche sur le traitement du cancer chez les enfants ? Cela représente des millions d'euros. On peut penser aussi aux multinationales, à des actions d'espionnage stratégique ou industriel.

Que faire ? Nous pouvons agir en citoyens sur nos données de santé

Cela commence par être pleinement conscient des risques encourus.

Ces risques sont idéologiques

Les GAFAM et autres géants du net propagent une idéologie :

- Le transhumanisme

  « Télécharger un cerveau humain signifie scanner tous les détails essentiels et les installer ensuite sur un système de calcul suffisamment puissant. Ce processus permettrait de capturer l'intégralité de la personnalité d'une personne, sa mémoire, ses talents, son histoire. » (*Humanité 2.0, la Bible du changement, 2007 de Raymond Kurzweil*). Raymond Kurzweil selon Wikipédia, conseiller de Google "pour apporter à Google la compréhension du langage naturel".

- Le solutionnisme
  Selon Eric Schmidt (Google) "*Si nous nous y prenons bien, je pense que nous pouvons réparer tous les problèmes de monde*" [12]
- Une conception US de la médecine fondée sur comportementaliste ce qu'illustre bien le DSM 5[13].

[11] [en ligne] Cyberattaques : « Les dossiers médicaux volés peuvent se revendre plusieurs millions d'euros sur le marché noir » selon Vincent Trély, expert en cybersécurité | Le Quotidien du Médecin (lequotidiendumedecin.fr) consulté le 12/4/2024

[12] https://www.lemonde.fr/blog/binaire/2021/11/16/odyssee-urbaine-autour-de-la-transition-numerique/#:~:text=%C2%AB%20Si%20nous%20nous%20y%20prenons,ex%C3%A9cutif%20de%20Google%2C%20en%202012 .

[13] https://psyclinicfes.files.wordpress.com/2020/03/dsm-5-manuel-diagnostique-et-statistique-des-troubles-mentaux.pdf

Le risque d'appauvrissement de la culture médicale

- Par la substitution à l'expertise clinique d'une conception métrique de la santé,
- Par l'exposition aux biais de l'IA :
  - biais liés à la programmation,
  - biais liés aux bases de données permettant d'entrainer l'IA,
  - l'IA doit savoir dire je ne sais pas ce qu'elle ne fait pas aujourd'hui.

La perte de souveraineté

Le *cloud act*[14] est une loi américaine qui permet notamment aux instances de justice américaines de solliciter auprès des fournisseurs de services opérant aux États-Unis, les communications personnelles d'un individu, citoyen ou résident US, sans que celui-ci en soit informé, ni que son pays de résidence ne le soit, ni que le pays où sont stockées ces données ne le soit.

Les risques éthiques

Le 13 mars 2024 dans un Rapport de la Commission de l'IA remis au Président de la République[15] on trouve parmi les 6 grandes lignes d'action celle de "*faciliter l'accès aux données*" : la notion même de « *donnée personnelle* », « *qui constitue la clé d'application du RGPD, suscite des interrogations dans un contexte croissant d'utilisation de données collectives* ». Les rapporteurs recommandent de "*supprimer les procédures d'autorisation préalable d'accès aux données de santé et de réduire les délais de réponse de la CNIL*".

Il faut aussi évoquer le risque de disparition de la personne derrière le profilage ce que décrit Antoinette Rouvroy (Chercheur qualifié, Centre de Recherche Information, Droit et Société, U. Namur) comme « derrière l'apparence d'hyperpersonnalisation le risque avec les big data d'épuiser la totalité du réel et donc des possibles ». Selon elle pour les big data : l'enjeu est moins la donnée personnelle que la disparition de la personne[16].

Risque de remise en cause du modèle social français

On est ici au cœur de l'affrontement entre la socialisation et l'individualisation.

Le régime de sécurité sociale français est fondé sur la mutualisation ce qui est l'assurance pour chaque bénéficiaire du régime de voir ses dépenses de santé prises en charge quelle que soit sa pathologie et quels que soient les coûts. A l'inverse la finalité d'un assureur privé est de traiter des risques individuels. S'agissant d'une entreprise commerciale l'objectif de l'assureur est de maximiser les gains et de minimiser les pertes avec pour conséquences le fait d'éliminer les clients présentant des risques de maladie importants.

La question de l'assurabilité dans le rapport assureurs/assurés n'est pas une vue de l'esprit pour rester dans l'actualité de ce printemps on peut évoquer les refus d'assurance qui commencent à se faire jour de la part des assureurs dans les zones du territoire qui sont ou ont été inondées[17].

---

[14] https://fr.wikipedia.org/wiki/CLOUD_Act

[15] https://www.info.gouv.fr/actualite/25-recommandations-pour-lia-en-france#:~:text=La%20Commission%20de%20l%27intelligence,%27intelligence%20artificielle%20(IA).

[16] Le Monde 22/1/2016 https://www.lemonde.fr/blog/binaire/2016/01/22/le-sujet-de-droit-au-peril-de-la-gouvernementalite-algorithmique/

[17] https://www.wedemain.fr/dechiffrer/desengagement-des-assureurs-quand-les-villes-doivent-assurer/

Comment agir ?

Agir pour la souveraineté du Système national des données de santé (SNDS)

Résultant de la loi du 24 juillet 2019 le SNDS[18] devrait reposer sur un Health data hub hébergé dans un cloud souverain.

Protéger nos données

Développer au plan individuel comme au plan collectif une éducation et une culture de la sécurité. : Il ne faut pas perdre de vue que les attaques qui aboutissent reposent souvent sur une défaillance une d'origine humaine. Il faut avoir conscience de ce qu'est l'ingénierie sociale et des méthodes qu'elles déploient (arnaque au président par exemple).

On pourra lire avec profit la publication de la CNIL : Guide de la sécurité des données personnelles : nouvelle édition 2024[19].

Rejoindre et soutenir des organisations tels que

- le Collectif Interhop : InterHop | Pour les logiciels libres, l'interopérabilité et l'utilisation auto-gérée des données de santé à l'échelle locale[20].

Créer de liens avec

- Associations de patients : France assos santé[21]
- CSF
- UNAF/UDAF
- Les associations du champ du handicap
- Et plus largement là partout où nous sommes présents

Proposer des solutions techniques

- Framasoft[22], Chatons[23], etc.

Développer un volet plaidoyer

- Framasoft
- Chatons

Conclusion

- L'intérêt du traitement numérique de l'information en santé n'est pas contestable, il ne saurait être question, évidemment, d'envisager un retour en arrière.
- Mais il ne va pas de soi, dans les sociétés « libérales », que la santé soit considérée comme un bien commun et non un bien marchand.
- Il nous faut considérer, avec Shoshana Zuboff que ce que nous vivons est de l'ordre du « sans précédent » et par conséquent non reconnaissable.
- Il nous faut donc agir :
    - Au plan individuel en développant et en promouvant la culture de la sécurité des données de santé,
    - Au plan collectif en défendant les acquis sociaux et en défendant notre souveraineté.

[18] https://www.snds.gouv.fr/SNDS/Qu-est-ce-que-le-SNDS
[19] https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles-nouvelle-edition-2024
[20] https://interhop.org/
[21] https://www.france-assos-sante.org/
[22] https://framasoft.org/fr/
[23] https://www.chatons.org/

- C’est dans ces conditions que l’on pourra instaurer un climat de confiance dans le traitement numérique de nos données de santé. Ce climat de confiance est la condition d’un bon fonctionnement du système de traitement numérique des données de santé.