



Données de santé, chevaux de Troie

Catégorie : **Mundus Numericus**

Tags : **Corps, Ethique, Loi, Plateforme, Politique, Société**

Personnages : **Annelore Coury, Yann Diener, Michel Foucault, Michel Gagneux, Dominique Pon**

21 décembre 2019

Le plan « *Ma santé 2022* » signe l'accélération du numérique dans le domaine de la santé. Nous relevons les risques qui accompagnent cet irréfutable progrès.

Dans une communauté d'intérêts, il y a danger dès qu'un membre devient trop puissant.

Jules Mazarin

Les nouvelles « données de santé »

Avant Mundus Numericus il y avait peu d'ambiguïté. Les « données de santé » correspondaient bien à ce que l'on imagine : résultats d'examens médicaux, informations concernant une pathologie, données corporelles... Elles restaient donc cantonnées dans les différents systèmes des professionnels de santé (cabinets médicaux, hôpitaux, laboratoires...). Mais on peut désormais obtenir des informations sur la santé en *croisant* entre elles d'autres types de données. Nous avons souvent évoqué cette caractéristique essentielle du milieu digital : tout est information, donc tout est nombre, donc tout est *commensurable* et n'importe quelle donnée acquiert une valeur inédite par le fait d'être ainsi devenue comparable et *corrélable* à n'importe quelle autre. Et surprise ! Ces

nouveaux croisements, utilisant des données éloignées du domaine de la santé, peuvent révéler assez précisément l'état de santé d'un individu.

Il y a cet exemple fameux, un peu ancien mais très éclairant. L'entreprise américaine de grande distribution Target avait développé en 2015 un modèle statistique permettant, en croisant les données d'achat des consommatrices sur une période assez longue¹, de savoir avant tout le monde qu'elles étaient enceintes² :

En analysant les données démographiques et historiques d'achat des millions de clients de Target, et toutes celles que l'enseigne a pu acheter auprès de prestataires spécialisés, les « data brokers », Andrew Pole [le statisticien de Target] a été en mesure d'identifier une liste de 25 produits que les femmes enceintes sont plus susceptibles d'acheter, jusqu'à pouvoir développer un « score de prévisibilité de grossesse » suffisamment précis pour savoir à quelques jours près à quel stade de sa grossesse la cliente se trouve quand elle passe à la caisse.

[...]

Imaginons une cliente de 23 ans qui vit à Atlanta et achète au mois de mars des pots de lotion cosmétique au beurre de cacao, et un sac assez grand pour pouvoir servir à transporter un nécessaire à langer, des suppléments alimentaires à base de zinc et de magnésium et un tapis bleu roi. Il y a 87% de chances qu'elle soit enceinte et l'accouchement programmé pour la fin du mois d'août.

Résultat : un homme a reçu à son domicile des bons de réduction de Target pour l'achat de produits destinés aux jeunes mamans. Il ignorait que sa fille de 16 ans était enceinte...

L'information « *achat d'un tapis bleu roi* », donnée anodine concernant un acte de consommation, a acquis par *destination* la valeur d'une donnée de santé après avoir été croisée avec des millions d'autres données. C'était il y quatre ans avec les seules données de Target et de quelques data brokers. Imaginons donc les diagnostics réalisables aujourd'hui avec les masses de données accumulées par les géants du numérique : heure de réveil, requêtes internet, achats en ligne, montre connectée, mails, etc.

Et depuis 2015 est apparu également ceci dont Andrew Pole ne disposait pas encore.

I.A. accélération

La chose la plus miséricordieuse en ce bas monde est l'incapacité de l'esprit humain à mettre en corrélation toutes les informations qu'il contient. [...] Un jour viendra où la synthèse de ces connaissances dissociées nous ouvrira des perspectives terrifiantes sur la réalité et la place effroyable que nous y occupons.

Howard Phillips Lovecraft – Le mythe de Cthulhu

¹ D'où l'intérêt stratégique des cartes de fidélité, l'un des plus vieux moyens de vendre nos données.

² Marc Sigrist pour Ozinzen – 16 décembre 2015 – [Un homme en colère car sa fille de 16 ans reçoit des publicités lui vantant des habits de bébé](#)

Les techniques dites d' « intelligence artificielle » (TIA) n'ont pas cette incapacité « miséricordieuse » et multiplient dramatiquement les destinations possibles en accomplissant des croisements massifs et inédits, au-delà des rêves de Target. Et nous voyons apparaître des corrélations incroyables, humainement imaginables, des capacités prédictives nouvelles, et tout ceci sans aucune théorie sous-jacente, sans effort conceptuel, seulement avec de la puissance technique brute. C'est la corrélation / prédiction à la portée de tous, notamment des milliers de startups qui inventent de nouvelles destinations pour nos données. C'est aussi une « révélation » : nous sommes (ou avons été rendus) très prévisibles... et comme disait le journaliste [Adam Curtis](#), « *les ordinateurs connaissent cet horrible secret* ».

Ajoutons que les TIA sont nourries par ces nouveaux capteurs de données *en temps réel* que sont les objets connectés : trottinette, vélo, montre, voiture, tensiomètre... De plus, leurs capacités de traitement d'images sont telles qu'elles peuvent analyser le visage, ses transformations et ses mouvements pour le diagnostic de troubles rares³ ou la détection des émotions⁴ etc. Nos enceintes connectées pourraient aussi détecter de légères altérations de la voix... Les « données de santé » par destination vont littéralement nous submerger.

Il est certain que les acteurs du numérique ayant accès à ces données et munis de ces techniques peuvent instantanément déduire notre état de santé et son évolution. Il n'est plus possible d'affirmer que telle donnée particulière (entrée dans un magasin, achat d'un tapis, parcours avec une trottinette, requête Google, photo...) n'aura pas un jour ou l'autre une destination médicale. Nos données sont *déjà stockées* par les objets que l'on nous propose *aujourd'hui* et peuvent attendre des années avant d'être croisées et de révéler d'autres horribles secrets.

Sisyphé

La sauvegarde de nos intérêts et de nos libertés impose donc en premier lieu l'élaboration de nouveaux textes normatifs s'appuyant sur une définition actualisée des « données de santé ». Mais comment faire ?

La Commission Nationale de l'Informatique et des Libertés (CNIL) a tenté l'exercice⁵. La difficulté est évidemment de tracer les contours d'un ensemble qui ne contiennent pas toutes les données imaginables (comme « *achat d'une lotion cosmétique au beurre de cacao* »). La CNIL tente de s'en sortir en précisant *ce que n'est pas* une donnée de santé (nous soulignons) :

N'entrent pas dans la notion de données de santé celles à partir desquelles aucune conséquence ne peut être tirée au regard de l'état de santé de la personne concernée (ex : une application collectant un nombre de pas au cours d'une promenade sans croisement de ces données avec d'autres).

³ Tempo Today – [L'intelligence artificielle pour le diagnostic de maladies rares en utilisant juste la photo du visage](#)

⁴ Jimmy Braun pour Blog Nutrition Santé – mars 2018 – [Lire les émotions à partir de changements minuscules dans la couleur du visage](#)

⁵ CNIL – [Qu'est-ce qu'une donnée de santé ?](#)

Et donc, à la rubrique questions / réponses :

Les données recueillies, en dehors d'un contexte médical (nombre de pas, poids, activité quotidienne...), par des outils de mesure de soi (montres, bracelets connectés, applications mobiles, etc.) sont-elles des données de santé ?

Tout dépend d'une part de la nature des données (un poids excessif peut révéler une obésité), d'autre part du croisement ou non de ces données à d'autres données révélant ainsi des informations sur l'état de santé de la personne.

C'est évidemment un impossible travail de Sisyphe, une définition qui ne peut jamais aboutir car toujours en retard sur les croisements à venir.

Il faut retenir de ce préambule sémantique que chaque fois qu'un texte parle de « donnée de santé », il y a une incertitude sur son domaine d'application. On pourrait donc s'attendre à une certaine prudence, si ce n'est de chacun d'entre nous tout au moins des autorités, au sujet de ces informations et destinations sensibles. Mais...

Convergence objective d'intérêts

En matière de déploiement des données de santé il y a une convergence objective d'intérêts entre l'individu préoccupé de sa santé, l'État qui déploie une politique et contrôle un budget, et bien entendu le secteur économique qui voit s'ouvrir de gigantesques débouchés.

Le secteur économique en particulier, assis sur un monceau de données à croiser, est en pleine ébullition : MedTech, e-santé, télémédecine, eHealthTech etc. avec à la clé⁶ : « *sauver des vies, améliorer la qualité des soins, diminution de la pression sur les structures médicales, prévention des problèmes, soins à domicile, confiance et engagement de tous pour la sécurité, création d'emplois et croissance économique...* ». Il y a des gains à la clé pour tous les acteurs et les applications MedTech sont innombrables et encouragées : diagnostic médical ; robot conversationnel et de soin ; montre connectée pour les patients épileptiques ; autotests médicaux et applications d'analyse ; monitoring (cloud et big data) et suivi de traitement des autistes ou autres personnes atteintes de désordres mentaux ; etc.

Ces applications permettent déjà une amélioration qualitative du système de santé (prévention, soin). Mais elles permettent aussi une réduction du coût total de ce système (moins d'hôpitaux, de médecins, d'infirmiers...). Et enfin, elles répondent aux besoins de l'individu lui-même, qu'il soit malade ou en bonne santé.

Il n'y a aucun doute : la e-santé constitue un authentique progrès pour tous.

En France

Le plan « Ma santé 2022 » répond au chant de ces sirènes de la e-santé et le chapitre intitulé « *Recourir au numérique pour mieux soigner* »⁷ expose des objectifs ambitieux :

⁶ Bizvibe - 2018 - [Top 20 Medtech Startups to Watch in 2018](#)

⁷ Ministère des Solidarités et de la Santé - 12 février 2019 - [Recourir au numérique pour mieux soigner](#)

« Déployer la télémédecine, S'appuyer sur le numérique pour améliorer les organisations et dégager du temps médical, Favoriser la production et l'utilisation des données de santé, Encourager l'innovation en e-santé... ».

Mais nous voyons poindre le problème. L'engagement fort de l'État pour l'utilisation massive des « données de santé » (au sens de la CNIL ?) engage sa responsabilité concernant l'usage de ces données. Il doit donc dans un même mouvement s'atteler à leur protection et « constituer une commission de l'éthique numérique en santé ». Évidemment la « schizophrénie » continue, celle d'un État de l'ordre ancien confronté au milieu digital sans avoir encore muté en « cyber-État » :

[...] le numérique devra tirer tous les bénéfices de l'intelligence artificielle dans le domaine de la santé tout en garantissant, sous la responsabilité de l'État, un haut niveau de sécurité et de confidentialité des données personnelles. C'est le rôle dévolu à la future plateforme des données de santé (« Health data hub »), qui modernisera l'exploitation des données à des fins de recherche et d'innovation.

Nous avons déjà relevé, dans le rapport [#FranceIA](#) du gouvernement précédent, cette impossibilité :

L'enjeu est d'arriver à protéger la vie privée tout en tirant parti du potentiel de l'IA qui suppose d'avoir accès à ces données.

Ce à quoi nous avons observé que « dans une économie d'acteur privés, il faut choisir ». Tout se joue, comme nous allons le voir, dans cet impossible « en même temps » : l'IA et la protection des données, l'accélération de la e-santé et la garantie d'une souveraineté française et européenne... La puissance des intérêts convergents est telle que le [système technicien](#), qui dispose déjà des solutions, avance sans attendre que nous ayons résolu ces contradictions. Nous contractons ainsi une sorte de « dette politique » que la seule jurisprudence à venir ne suffira pas à rembourser.

Hébergeurs de données de santé

La première étape consiste à identifier des acteurs du numérique capables de faire avancer au pas de charge tout le secteur français de la santé. Compte tenu de la sensibilité des « données de santé » (au sens de la CNIL ?), il n'est évidemment pas question de laisser faire n'importe quoi à ces acteurs, appelés « Hébergeurs de Données de Santé » (HDS), qui doivent désormais être *certifiés*⁸. Une fois la « certification » acquise et ainsi parés de l'étendard, ces hébergeurs deviennent insoupçonnables. Et sous nos yeux réellement ébahis nous trouvons les grands acteurs américains du numérique parmi la soixantaine de HDS à ce jour : Microsoft, Google, Amazon, IBM, Salesforce... ! Ce processus de certification était pourtant une occasion unique de récupérer un peu de souveraineté numérique. Mais les bénéfices immédiats excèdent de loin les inconvénients futurs (la dette qu'il faudra rembourser).

⁸ ASIP Santé – [Liste des hébergeurs certifiés](#)

N'importe quelle structure de santé (hôpital, médecin...) peut donc traiter nos informations médicales, les plus sensibles qui soient, dans les systèmes et par les IA de Microsoft ou de Google, par exemple, puisqu'ils sont « certifiés ». Nous allons donner un aperçu de ce que « certification » veut dire dans ce cas et comment nous en sommes arrivés là. Mais auparavant, il a fallu préparer les esprits.

Historique et rhétorique

Les gouvernements successifs ont depuis longtemps la « vision » d'un système de santé organisé autour du patient et non pas exclusivement autour des lieux de diagnostic et de soin. Ce renversement doit s'appuyer sur des dispositifs techniques intégrés et partagés par tous les acteurs de la santé.

C'est la raison pour laquelle l'Agence pour les Systèmes d'Information Partagés de Santé (ASIP Santé) a été créée en 2009 sur proposition de Michel Gagneux, haut fonctionnaire, énarque (de la fameuse promotion Voltaire), et qui a fait l'essentiel de sa carrière à l'IGAS, l'Inspection Générale des Affaires Sociales. L'ASIP Santé, comme son nom l'indique, est une structure opérationnelle en charge de promouvoir l'harmonisation des systèmes des organismes de santé et fut le maître d'ouvrage du Dossier Médical Partagé (DMP). On doit également à Michel Gagneux la création d'une instance de supervision au sein du Ministère : la Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS)⁹.

Malgré ces avancées, le rapport Pon-Coury de 2018 (« *Accélérer le virage numérique* »¹⁰) souligne encore le « *manque de structuration de la gouvernance autour du numérique de santé en France* ». Ce rapport est particulièrement instructif de la « philosophie » qui règne actuellement en matière de e-santé en France (et de e-choses en général) et dont nous pouvons relever deux symptômes caractéristiques.

En premier lieu, l'une des lignes directrices consiste à « *sortir d'une vision d'un patient « objet » de soins pour aller vers un usager « acteur » de sa santé* ». Ce propos, s'il semble inspirant et désigne un avenir tentant, véhicule un élément essentiel de la doxa numérique : *l'individu doit s'autonomiser*. Cela signifie en réalité qu'il devient le centre d'un ensemble de relations numérisées qui convergent vers lui et finissent par le déterminer. D'autonomie il ne faut plus rêver¹¹. On ne compte plus les services, publics ou privés, les applications commençant par « *mon...* », « *my...* » et nécessitant dans tous les cas, sous les atours d'une fausse liberté, une intermédiation experte ou technique, souvent obscure, source de nouveaux pouvoirs (Uber, Amazon etc.), quand ce n'est pas une onction gouvernementale dans les États les plus « cyber » ([Chine](#)).

Second signe des temps, il faut créer une « *commission dédiée à l'éthique au sein du comité stratégique du numérique en santé* ». Nous ne doutons pas qu'il faille quelque chose comme une « métaréflexion » sur le sens et les impacts de ce que nous envisageons (ce que nous tentons d'ailleurs ici même). Mais il s'agit ici plutôt ici d'un simple étendard

⁹ DH Magazine 154 – 2016 – [La santé à l'ère numérique – Entretien avec Michel Gagneux, Directeur de l'ASIP Santé](#)

¹⁰ Ministère des Solidarités et de la Santé – 2018 – [Rapport final « Accélérer le virage numérique »](#)

¹¹ Nous avons décrit ce phénomène dans l'article [PageRank, Parcoursup et autres machines morales](#) (chapitre « Machines morales, objets, relations »).

« éthique » à dresser chaque fois que la confiance des usagers risque de flancher, avec à la clé toujours le même problème : c'est celui qui risquerait de manquer à une certaine éthique qui crée et anime les « comités d'éthique ». Et ainsi on propose un « processus de labellisation ou de certification éthique », de « sensibiliser le grand public sur les sujets d'éthique en e-santé », voire de « dynamiser la recherche en matière d'éthique du numérique en santé ... Mais Dominique Pon et Annelore Coury, aussi bien intentionnés soient-ils, ne seront pas entendus ou si peu.

La technocratie en action

Une fois l'autonomie et l'éthique « traitées », la technocratie peut s'ébranler.

On soulignera donc à juste titre, comme Michel Gagneux à l'époque, que les systèmes d'information du système de santé français ne sont pas « *interopérables* ». Ceci signifie que les données de santé ne peuvent pas circuler facilement d'un environnement à un autre. Il faudra donc (nous soulignons) « *fédérer les acteurs institutionnels, publics et privés au service des usagers du système de santé : l'Espace Numérique de Santé* » :

Il s'agira d'un compte personnel unique, créé dès la naissance pour chaque citoyen, donnant accès à un portail personnalisé de services ainsi qu'à des applications de santé référencées. Il sera accessible sur tous supports (smartphone, ordinateur, tablette, borne interactive, ...) et permettra à chaque usager de gérer l'ensemble de ses données personnelles de santé ainsi que tous ses services numériques de santé.

C'est aussi simple que cela ! Dans Mundus Numericus, les textes des projets, quels que soient les sujets, sont interchangeable. Ainsi grâce à ce « portail », notre avatar numérique sera complet et permettra semble-t-il de « *faire de l'utilisateur [...] un acteur de son parcours de santé tout au long de sa vie en lui permettant de co-construire ce parcours en interaction avec les professionnels, les structures et les institutions de santé* ».

Nous ne commenterons pas davantage les éléments de ce rapport pour le moins ambigu, mais l'Espace Numérique de Santé tel qu'il est envisagé signe la ruée des acteurs privés vers cette manne absolue : le croisement et la marchandisation des « données de santé », quelles qu'elles soient.

Chevaux de Troie

Sous couvert d'éthique, d'autonomie de l'utilisateur (qui sera, soit dit en passant, plus que jamais enchaîné à sa propre « hypocondrie », vu le succès des sites de santé ou des applications de « *quantified self* »), de chartes, de garanties de sécurité, de confidentialité, etc. on promet un système numérique de santé moderne et qui servira les intérêts des pouvoirs publics, des acteurs économiques et de chacun d'entre nous. Il faut aller vite. En matière de sécurité notamment, il faudra donc s'appuyer sur des acteurs *existants* capables de garantir à la fois la « *scalabilité* », la capacité technique d'un système à se déployer massivement, et une *sécurité* maximale pour protéger ces données sensibles de toute utilisation malveillante. Ces acteurs, nous les connaissons.

En mars 2018, dans l'article L'[IA par ses ombres](#), nous avons déjà relayé une conclusion essentielle d'une étude consacrée aux usages malveillants de l'intelligence artificielle (paragraphe « *Winners take even more...* »). Nous la reproduisons ici :

Les géants de la tech et des médias peuvent devenir des havres de paix technologiques pour les peuples car, par leur accès à des données pertinentes sur une échelle massive, par leur maîtrise des produits et des canaux de communication, ils sont dans la position hautement favorable de pouvoir offrir à leurs usagers la protection adéquate.

CQFD ! Pour devenir Hébergeur de Données de Santé aujourd'hui, il faut se faire certifier par un organisme *de son choix* qui procédera, à quelques détails près, à la certification essentiellement sur la base de normes de sécurité de systèmes d'information *existantes* (ISO 27001, ISO 20000...). Personne n'a pris le temps d'établir « de zéro » un référentiel de certification réellement propre aux données de santé, au bénéfice de notre souveraineté, et qui aurait exigé pour le coup une véritable réflexion de société. C'est ainsi que les « *géants de la tech et des médias* » apparaissent dans la liste des HDS, déjà scalables, déjà conformes (à quelques détails près) aux normes techniques et organisationnelles de sécurité les plus exigeantes. Voici comment Microsoft, Amazon, Google et d'autres américains se sont trouvés adoubés en un an à peine.

Winners take even more... grâce au « cheval » d'une rhétorique bien rôdée et déployée semble-t-il à l'insu même de leurs auteurs, à la manière d'une novlangue.

Ce que risquent les « troyens »

Il y a trois risques principaux.

Premièrement il y a, comme nous l'avons relevé, l'épée de Damoclès du croisement *abusif* des données malgré les garanties d'éthique, de protection des données à caractère personnel (RGPD), de choix du consommateur... Ces garanties seront difficiles à défendre pour au moins deux raisons. D'abord, *la recherche et l'innovation* : personne ne pourra s'opposer longtemps à des croisements permettant de meilleurs soins ou une meilleure prévention. Ensuite, *la concurrence mondiale*. Aucune entreprise française ou européenne ne pourra, à terme, rester compétitive face à des concurrents américains ou chinois qui innoveront sans cesse et *personnalisent* leurs services sur la base du croisement déjà possible, déjà si efficace, de nos données pour déduire notre état de santé : assurances, services bancaires, habillement... Les exemples sont déjà nombreux et les grands acteurs du numérique avec leurs services d'intelligence artificielle déjà prêts à être utilisés sont aux premières loges pour équiper ces entreprises.

Ainsi, dans un pays plus libéral que le reste de l'Europe et sur le point de larguer les amarres, le Royaume-Uni, Amazon vient de remporter une bataille décisive. La voie est tracée et l'Europe aura toutes les difficultés à défendre sa singularité (nous soulignons)¹² :

¹² Arnaud Pagès pour Korii – 12 décembre 2019 – [Le gouvernement britannique autorise Amazon à accéder aux données de 40 millions de patients](#)

Privacy International, une ONG qui milite contre la violation de la vie privée commise par les gouvernements, a révélé, après enquête et publication de l'intégralité du contrat, qu'il incluait « toutes les informations sur les soins de santé », y compris, sans s'y limiter, les symptômes, les causes et les définitions, ainsi que tout le contenu, les données, les informations et autres documents protégés par le droit d'auteur», détenus par le NHS et le ministère de la Santé et des Affaires Sociales. Le mastodonte du e-commerce a par ailleurs reçu un blanc-seing pour utiliser ces données à d'autres fins que de fournir des conseils médicaux.

L'histoire de Target nous revient en mémoire. Dans le cas d'Amazon : à la puissance mille.

Deuxièmement, il y a bien évidemment le piratage de données. Aucune norme de sécurité, aussi ISO soit-elle, ne peut garantir contre une fuite. Il suffit de se pencher pour ramasser des exemples de piratage et dans The Conversation, Nathalie Devillier fait une très bonne synthèse de la situation (notamment concernant les objets connectés, vulnérables auxiliaires du [milieu naturel digital](#) indispensables à notre future e-santé)¹³ :

La situation est très alarmante avec un nombre d'attaques par rançongiciel qui pourrait quadrupler dans le secteur de la santé d'ici 2020. Les plus grandes entreprises ne sont pas à l'abri d'un scandale résultant d'un piratage. Quand bien même l'hébergement des données de santé des Français reste soumis à une procédure d'approbation de l'entreprise par le ministère de la Santé, cela ne garantit nullement la réactivité de celle-ci face à un bug voire à une attaque.

Nous sommes prévenus.

Il y a enfin ce troisième risque qui taraude tous les juristes et spécialistes de la sécurité en Europe : le « *CLOUD Act* » américain¹⁴. Cette loi fédérale facilite l'obtention, par les forces de l'ordre américaines, de données stockées à l'étranger. Elle s'applique à tout fournisseur de services américain (donc Microsoft, Amazon, Google, etc.) quand bien même les données en question concerneraient des citoyens européens et seraient hébergées sur des serveurs en Europe :

Cette loi permet notamment aux forces de l'ordre américaines d'obtenir les données personnelles d'un individu 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.

Il faudrait un article entier pour développer ce dernier risque mais nous devons désormais savoir que pèse un risque supplémentaire sur nos données de santé hébergées par des acteurs américains.

Ouverture sur le corps numérique

Le cas des données de santé illustre assez bien le cycle naturel du système numérique, dont le mouvement démarre par une convergence objective d'intérêts publics et privés

¹³ Nathalie Devillier pour The Conversation – 14 décembre 2019 – [Santé et objets connectés : le risque de piratage, fantasme ou réalité ?](#)

¹⁴ Wikipédia – [CLOUD Act](#)

(la e-santé consiste en soi un authentique progrès) mais accélère ensuite de façon technocratique, couvert par une rhétorique de l'éthique et de l'autonomie, et finit par désigner toujours les mêmes gagnants. Nous payons ce mouvement en nous « endettant » socialement (les futures oppositions), politiquement (les coûts de l'abandon de souveraineté) et techniquement (les futurs scandales de piratage)... et il est impossible de savoir si cette dette correspond à un investissement « rentable ».

Pour finir, ce passionnant sujet des données de santé soulève une question essentielle, tant juridique que philosophique : celle de la *nature* de nos données et de leur *propriété*. En effet, les informations numériques qui nous concernent sont tellement nombreuses et croisées qu'elles finissent par définir un « pseudo-corps numérique », dont on peut déterminer l'état de santé, et donc assez déterminant pour notre condition dans un (futur) cyber-État. Or, aujourd'hui, les « organes » de ce « corps numérique » ne nous appartiennent pas et ce corps n'est même pas (re)constitué. Est-il donc possible d'envisager une innovation radicale, un *corps numérique* pour chacun, techniquement intègre, protégé et intime, légalement défini et respecté ? Le corps d'un cyber-citoyen qui pourrait faire *barrage*.

Post-scriptum : au sujet du « biopouvoir »

On aurait tort de négliger les tensions souterraines à la jonction de ces deux « plaques » : la technostructure d'un côté, dont nous venons de décrire quelques manifestations, et certaines formes d'aspirations à la « liberté » auxquelles il manque de la cohérence pour gagner le « centre ». Si les avancées en matière de santé semblent s'accomplir sans heurts, en réalité certains esprits plus concernés ou plus clairvoyants commencent à se faire entendre.

Car cette technostructure sert une forme nouvelle et encore mal déterminée de ce que le philosophe Michel Foucault avait appelé le « *biopouvoir* » animé par une « *biopolitique* »¹⁵ (ajout entre crochets) :

[Foucault] relève que ce nouveau type de pouvoir prend en compte et s'exerce sur le corps et sur la vie, à la différence du plus ancien qui s'appliquait, selon le modèle juridique, sur les sujets. [...] Foucault va tantôt mettre l'accent sur la prise en compte de la vie, et développer la genèse de la biopolitique, tantôt souligner la surveillance individualisante, et mettra en avant l'émergence du pouvoir disciplinaire [écoles, hôpitaux, prisons, camps...] .

La biopolitique serait pour Michel Foucault, l'action concertée de la puissance commune sur l'ensemble des sujets, en tant qu'êtres vivants, sur la vie de la population, considérée comme une richesse de la puissance commune [technostructure publique / privée], devant être l'objet d'attention en vue de la faire croître et d'en accroître la vitalité [et donc l'efficacité économique] .

¹⁵ Wikipédia – [Biopolitique](#)

Nous ne développerons pas ce sujet dans un bref post-scriptum. Il s'agit seulement de ranger ce concept dans notre « todo list ». En attendant d'y travailler, il nous permet d'introduire un quatrième risque, celui de l'*aléa politique*. Commençons par un exemple. Dans un court article paru dans Charlie Hebdo en mai dernier, le psychanalyste Yann Diener évoque un décret passé relativement inaperçu (ajouts entre crochets)¹⁶ :

[...] un décret a été signé le 7 mai dernier pour autoriser une « mise en relation » [croisement] du fichier des personnes radicalisées (FSPRT) avec le fichier des patients hospitalisés en psychiatrie sans consentement (le déjà très controversé Hopsyweb). Toutes les organisations de soignants et de patients « psy » sont vent debout contre ce décret signé par la ministre de la Santé.

La tentation des croisements n'est pas réservée au secteur commercial (cf. la [Chine](#)) et elle se justifie en France comme ailleurs, désormais, par une sorte d'« état d'exception » rampant et permanent qui tend à devenir la règle (cf. par exemple nos dissertations sur [François Sureau](#) ou sur les [fake news](#)). Le quatrième risque est donc l'attentat à nos libertés.

Yann Diener envisage ce problème comme une manifestation du « *biopouvoir* » et utilise donc ce concept politiquement. C'est donc devenu une affaire d'opinion plus que de philosophie. D'ailleurs, le concept de « *biopouvoir* », comme celui de « [système technicien](#) » proposé par Jacques Ellul, est en général utilisé par les contempteurs de la technique. C'est tout à fait dommage car ils ont une indéniable utilité analytique pour lire Mundus Numericus.

C'est donc à une actualisation du concept de « *biopouvoir* » qu'il faudrait procéder en dépassant notamment ses exemplifications classiques par la biologie (en particulier la génétique) ou par ses manifestations les plus monstrueuses (les camps de concentration). Il faut maintenant interroger le nouvel environnement numérique, que Foucault ne connaissait pas (et qu'Agamben semblait à peine deviner), et les prises offertes à un nouveau « cyberbiopouvoir » : les informations. Un retour du concept en politique pourrait dès lors s'accomplir de façon bien plus efficace.

¹⁶ Yann Diener pour Charlie Hebdo – 29 mai 2019 – [1969-2019 l'essor du biopouvoir](#)