Organisation des Nations Unies pour l'éducation, la science et la culture

Comité international de bioéthique (CIB)

SHS/YES/IBC-24/17/3 REV.2
Paris, le 15 septembre 2017
Original : anglais

RAPPORT DU CIB SUR LES MÉGADONNÉES ET LA SANTÉ

Dans le cadre son programme de travail 2016-2017, le Comité international de bioéthique (CIB) de l'UNESCO a choisi de se pencher sur la problématique des mégadonnées dans le domaine de la santé, en abordant notamment les questions de l'autonomie, du consentement, de la protection des données et de la gouvernance.

Lors de sa 22e session (ordinaire) tenue en septembre 2015, le CIB a mis en place un groupe de travail chargé de mener une première réflexion sur le sujet. Un document préparatoire a été rédigé entre octobre 2015 et mai 2016, au moyen d'échanges de courriels. Le groupe de travail s'est ensuite réuni à Cologne en mai 2016 afin de parachever la structure et la teneur du document. Le groupe de travail du CIB s'est appuyé sur ces travaux pour élaborer un projet de rapport préliminaire, qui a fait l'objet d'un débat lors de sa 23e session (ordinaire), en septembre 2016. À la suite de cette discussion, il a procédé à une révision du projet de rapport préliminaire entre septembre et décembre 2016. Il s'est ensuite réuni en Espagne en mars 2017 afin de parachever ce document. Une version révisée du projet de rapport a été soumise pour observations au Comité intergouvernemental de bioéthique (CIGB), au CIB et à la Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST) entre mai et juin 2017. Le projet de rapport final a été ensuite révisé en fonction des commentaires reçus. Ce projet final du rapport a été ensuite examiné et révisé lors de la 24e session (ordinaire) du CIB, et il a été adopté par le Comité le 15 septembre 2017.

Le présent document ne prétend pas être exhaustif et ne représente pas nécessairement le point de vue des États membres de l'UNESCO.

RAPPORT DU CIB SUR LES MÉGADONNÉES ET LA SANTÉ

I. PORTÉE ET DÉFINITIONS

II. RÉGLEMENTATION JURIDIQUE

III. VISIONS, TENDANCES ET DÉFIS

IV. ASPECTS ÉTHIQUES

- **IV.1. Autonomie et consentement**
- **IV.2. Confidentialité et respect de la vie privée**
- **IV.3. De la propriété à la conservation et au partage des bienfaits**
- **IV.4. Justice**
  - **IV.4.1. Fracture numérique**
  - **IV.4.2. Non-discrimination**
- **IV.5. Durabilité énergétique et environnementale**
- **IV.6. Recherche**

V. GOUVERNANCE

VI. RECOMMANDATIONS

BIBLIOGRAPHIE

RAPPORT DU CIB SUR LES MÉGADONNÉES ET LA SANTÉ

I. PORTÉE ET DÉFINITIONS

1. Le phénomène des mégadonnées, c'est-à-dire la numérisation des données à très grande échelle, ne cesse de prendre de l'ampleur. Les mégadonnées touchent désormais à tous les aspects de la vie humaine, partout dans le monde, et donnent naissance à de profonds changements. Dans ce rapport, le CIB se penche sur les questions relatives au domaine de la santé au niveau individuel et public. Il présente des propositions visant à exploiter pleinement le potentiel des mégadonnées, dans le respect de la dignité humaine, des droits de la personne et des libertés fondamentales, tel qu'énoncé à l'article 3 de la Déclaration universelle sur la bioéthique et les droits de l'Homme (2005).

2. Les mégadonnées se distinguent par les cinq critères suivants (les « cinq V ») :

   a. Le *volume* se rapporte à l'énorme quantité de données numériques qui augmente de manière exponentielle. En 2000, les trois quarts des données étaient analogiques ; aujourd'hui, les données numériques représentent 99 % de la masse des données. Selon les estimations, elles devraient atteindre 44 zettaoctets (10^{21}) d'ici à 2020 et 180 zettaoctets à l'horizon 2025 (Centre international de données [CID], 2014). Notons toutefois que le volume de données (par exemple le volume des données issues du séquençage du génome) ne suffit pas à définir le phénomène des mégadonnées.

   b. La *variété* se rapporte à la diversité des types et des sources de données. Les données relatives aux soins de santé et à la recherche médicale proviennent de multiples sources : prise en charge médicale des patients ; données de santé publique ; données des systèmes d'assurance ; données de recherche recueillies par les chercheurs, les scientifiques citoyens[1], les entreprises et les particuliers ; et données sur le mode de vie (elles peuvent être par exemple des applications mobiles de santé, réseaux sociaux et commerce). Ces données peuvent être classées selon des modalités et des critères différents (données personnelles, ou des données anonymes, elles peuvent être primaires, ou secondaires ou des métadonnées).

   c. La *vitesse* se rapporte à la très grande vitesse à laquelle les données sont recueillies et traitées. Le suivi en temps réel et la technologie du *cloud* permettent de traiter globalement les données en quelques secondes, voire d'en tirer instantanément des recommandations (traitement, comportement, nutrition, etc.).

   d. La *validité* se rapporte à la qualité des données et à leur fiabilité, c'est-à-dire la pertinence de leur contenu et leur degré de précision. Le contexte des données constitue à ce titre un élément important.

   e. La *valeur* se rapporte à l'utilité des données dans un cadre spécifique, par exemple une maladie. Là encore, le contexte des données doit être pris en compte.

3. Le CIB utilise le terme « mégadonnées » dans le domaine de la santé pour désigner le recueil de grands volumes de données complexes liées à la santé qui proviennent de sources multiples. Généralement, ces ensembles de données concernent un très grand nombre de personnes, toutefois, l'analyse de toutes les données relatives à un seul patient dans certaines conditions peut également être considérée comme une analyse de mégadonnées.

[1] Aux fins du présent rapport, le terme « science citoyenne » se rapporte aux projets de recherche menés par des personnes non spécialistes, souvent en coopération avec des scientifiques et des institutions de recherche, ou sous leur supervision.

4. Les mégadonnées ne peuvent être traitées au moyen des technologies traditionnelles, mais requièrent une puissance de calcul supérieure et l'élaboration de nouveaux algorithmes. Chaque type d'algorithme présente des enjeux éthiques qui lui sont propres. Il existe par exemple des algorithmes dédiés à une tâche donnée, qui sont programmés en séquence définie d'opérations précises et qui garantissent donc une transparence technique. Inversement, il existe des algorithmes d'intelligence artificielle, d'apprentissage automatique et d'apprentissage profond pour lesquels il est difficile d'assurer la transparence, car ils apprennent grâce à de grandes séries de données et exécutent des opérations plus ou moins « par eux-mêmes ».

5. Il n'existe pas de définition universelle de la santé applicable à tous les contextes, à tous les stades de la vie et dans toutes les régions du monde. Les définitions varient selon la perspective (compréhension subjective ou notion objective) et leur finalité, selon qu'il s'agit d'actions thérapeutiques et/ou préventives qui peuvent avoir leur légitimité. Par exemple, l'Organisation mondiale de la Santé (OMS) définit la santé comme « un état de complet bien-être physique, mental et social [qui] ne consiste pas seulement en une absence de maladie ou d'infirmité ». Cette vaste définition, qui s'étend à tous les aspects de la vie humaine, a une valeur prescriptive et sert de fil directeur à la promotion de la santé dans le monde. Lorsque les systèmes de santé nationaux doivent préciser et circonscrire les responsabilités des professionnels et des institutions de la santé, une approche plus précise et ciblée est utilisée.

6. La définition de l'OMS indique que dans la vie tout est lié à la santé. En ce sens, elle valide une approche globale de la santé et estompe la distinction entre santé au sens médical et mode de vie. Les mégadonnées offrent la possibilité technique d'appuyer cette conception holistique, tout en suscitant de vives inquiétudes quant à la protection des droits de l'Homme.

7. Portés par les technologies de l'information et de la communication (TIC), de nouveaux termes, tels que santé mobile ou cybersanté, ont fait leur apparition. L'OMS définit la cybersanté comme « l'utilisation des TIC au service de la santé » (OMS, n.d.) et la santé mobile comme une sous-composante de la cybersanté, qui vise « les prestations de soins médicaux et de santé publique effectuées à l'aide d'appareils mobiles, tels que les téléphones portables, les moniteurs, les assistants numériques personnels, et autres appareils sans fil » (OMS, 2011).

8. Le nombre d'applications dédiées à la santé ne cesse d'augmenter. Il semblerait qu'il en existe plus de 300 000 à l'heure actuelle. On distingue trois grandes catégories : les applications liées à la prise en charge, celles liées à la prévision et à la prévention, et enfin celles liées au mode de vie. Le contrôle de toutes ces applications et la garantie de leur qualité relèvent de l'impossible. Il est en tout état de cause extrêmement difficile de distinguer précisément celles qui relèvent — ou non — du champ médical. Pour cette raison, notre approche des mégadonnées et de la santé ne se limite pas à la recherche médicale et aux soins de santé traditionnels.

II. RÉGLEMENTATION JURIDIQUE

9. Les cadres juridiques nationaux et internationaux ne prévoient aucune disposition spécifique concernant les mégadonnées. Toutefois de nombreuses juridictions, notamment en Europe, possèdent un cadre réglementaire détaillé régissant la protection des données personnelles. Leurs dispositions peuvent fréquemment s'appliquer aux mégadonnées, bien que leur quantité, leur analyse, leur accessibilité et leur application soient sans précédent. Par ailleurs, même en l'absence de loi spécifique sur la protection des données personnelles, les pays peuvent s'appuyer sur le droit constitutionnel, le droit écrit et le droit coutumier dans le même but. C'est le cas notamment de la plupart des pays de la Communauté d'États indépendants (CNUCED, 2016). La réglementation ne fait donc pas défaut. En revanche, il conviendrait d'établir des dispositions — voire des principes — spécifiques afin de réglementer les nouvelles propriétés des mégadonnées.

10. S'agissant du cadre juridique international, l'article 12 de la Déclaration universelle des droits de l'Homme, adoptée par l'Assemblée générale des Nations Unies en 1948, porte sur la protection de la vie privée et dispose : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes » (Nations Unies, 1948). Dans la même veine, l'article 8, paragraphe 1 de la Convention européenne des droits de l'Homme dispose : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance » (Conseil de l'Europe, 1950). Le paragraphe suivant précise : « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui » (Conseil de l'Europe, 1950).

11. Une grande partie de la réglementation internationale a coïncidé avec l'apparition des flux de données internationaux, dus principalement à la commercialisation des prestations de santé, laquelle implique l'échange transfrontière de données. À cet égard, la Conférence des Nations Unies sur le commerce et le développement (CNUCED) a publié en 2016 une étude importante sur la réglementation de la protection des données et les flux de données internationaux (*Data protection regulations and international data flows*). Les *Principes directeurs pour la réglementation des fichiers personnels informatisés* de l'Assemblée générale des Nations Unies publiées en 1990 ont permis d'obtenir un consensus sur les points fondamentaux. Ce texte fixe notamment les principes de finalité et de sécurité en vue de garantir un niveau minimal de confidentialité et de protection de la vie privée dans les législations nationales. En outre, les pays doivent désigner une autorité chargée de veiller au respect de ces principes, de sanctionner les contrevenants et, le cas échéant, d'ordonner des mesures de protection de la vie privée lors des échanges transfrontières de données personnelles. Les directives devaient s'appliquer en premier lieu aux fichiers contenant des données personnelles, qu'ils soient informatisés ou traités manuellement (voir paragraphe 10 desdites directives). Toutefois, elles peuvent s'appliquer, dans une certaine mesure, aux mégadonnées. Deux autres textes non contraignants ont contribué à orienter les cadres juridiques nationaux : la *Déclaration de l'AMM sur les considérations éthiques concernant les bases de données de santé et les biobanques* (2016) et la *Déclaration d'Helsinki* (2013) de l'Association médicale mondiale. Les principes directeurs en matière de protection des données adoptés par la plupart des juridictions nationales et des régimes internationaux font l'objet d'un vaste consensus. La principale difficulté réside dans l'hétérogénéité de leur mise en œuvre et du détail des législations nationales sur la protection des données (CNUCED, 2016).

12. L'Organisation de coopération et de développement économiques (OCDE) a publié des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* (révisées en 2013). En 2010, l'OCDE a également publié un rapport dans lequel elle souligne la nécessité d'encadrer juridiquement le partage des données (OCDE, 2010). La mise en place d'un nouveau cadre juridique régissant le partage de données sur la santé est nécessaire si l'on veut faciliter les échanges transfrontières, interorganisationnels et interprofessionnels (dans et entre les organismes de santé). Selon l'étude, très peu de membres de l'OCDE ont pris des mesures concrètes en ce sens. Plus récemment, en janvier 2017, l'OCDE a publié des recommandations sur la gouvernance des données de santé (*Recommendation on Health Data Governance).* Celles-ci soulignent l'importance de renforcer la protection légale des données à travers l'éducation et la sensibilisation, le développement des compétences et la promotion de mesures techniques. Elles appellent les pays à élaborer et mettre en œuvre des cadres régissant la gouvernance des données de santé qui garantissent la protection de la vie privée tout en permettant l'utilisation des données de santé d'intérêt public conformément à douze principes directeurs.

13. Les réglementations européennes et américaines présentent une différence importante. Pour les Européens, la vie privée constitue un droit de l'Homme fondamental qui suppose une réglementation descendante ainsi que des dispositions dotées d'une portée générale, limitant l'utilisation des données ou exigeant un consentement explicite. Les États-Unis, en revanche, privilégient une réglementation sectorielle axée sur les risques liés à la protection de la vie privée dans un domaine particulier (santé, crédit, etc.). Les règles générales sur l'utilisation des données sont donc moins nombreuses, une façon d'encourager l'industrie à faire preuve d'innovation dans ses produits et ses services. De plus, certaines utilisations potentielles des informations, qui ne sont rattachées à aucun secteur, ne sont pas réglementées (États-Unis, 2014).

14. Dans ce contexte, le ministère américain du Commerce, la Commission européenne et le gouvernement suisse ont élaboré des cadres régissant la protection des données personnelles entre l'Union européenne (UE) et les États-Unis et entre la Suisse et les États-Unis (Privacy Shield), afin de garantir le respect des exigences en la matière dans le cadre des échanges commerciaux transatlantiques (États-Unis, n.d.). Le « bouclier » de protection des données a remplacé les « Principes de la sphère de sécurité » (Safe Harbour Privacy Agreement) adoptés en 2000, et fait l'objet de révisions annuelles afin qu'il soit en phase avec les évolutions technologiques et la mutation du régime européen (voir paragraphe 27 ci-dessous) (Weiss et Archick, 2016).

15. Le Conseil de l'Europe a adopté en 1981 la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* visant à protéger les personnes physiques des abus associés à la collecte et au traitement des données personnelles. En 2001, le Conseil a adopté le Protocole additionnel à ladite Convention concernant les autorités de contrôle et les flux transfrontières de données. Il prévoit l'établissement d'autorités de contrôle chargées d'assurer le respect des lois ou règlements introduits par les États en application de la Convention. Par ailleurs, les données ne pourront être transférées que si elles bénéficient dans l'État ou l'organisation internationale destinataire, d'un niveau de protection adéquat. En 2017, les Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées ont été établies sur la base de cette Convention.

16. L'UE ne possède qu'une compétence juridique limitée en matière de santé, essentiellement afin de promouvoir la coopération et la coordination entre les États membres. Il existe cependant un texte collectif en matière de protection des données, la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (UE, 1995). Les choses vont changer en 2018. La directive actuellement en vigueur sera remplacée par un règlement directement contraignant pour tous les États membres et qui s'appliquera également aux sociétés non européennes (UE, 2016).

a. Le nouveau règlement européen dispose que « [l]e traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux. Le présent règlement respecte tous les droits fondamentaux, les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, ainsi que la diversité culturelle, religieuse et linguistique » (UE, 2016, paragraphe 4).

b. Le règlement dispose également que « le consentement devrait être donné par un acte positif clair. (…) Si le consentement de la personne concernée est donné

à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé » (paragraphe 32), ajoutant que « [l]e consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice » (UE, 2016, paragraphe 42).

c. S'agissant de la recherche, le règlement précise que « dans le respect des normes éthiques reconnues en matière de recherche scientifique[,] [l]es personnes concernées devraient pouvoir donner leur consentement (…) pour ce qui est de certains domaines de la recherche [scientifique] », dans la mesure où « [s]ouvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel (…) au moment de la collecte des données » (UE, 2016, paragraphe 33).

d. En ce qui concerne la santé publique, « [l]e traitement des catégories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques » (UE, 2016, paragraphe 54).

17. Les États-Unis ont récemment adopté plusieurs textes en vue d'établir un cadre juridique. Bien qu'il n'existe aucune réglementation relative aux mégadonnées, les entreprises chargées du traitement des mégadonnées médicales doivent se conformer à la réglementation sur la protection des données applicable à l'échelle fédérale, à savoir le Health Insurance Portability and Accountability Act (HIPAA) (loi sur la transférabilité et la responsabilité de l'assurance maladie) et la Privacy Rule, la règle afférente relative à la protection des données médicales (États-Unis, 1996 ; États-Unis, 2002). Ceux-ci doivent être complétés par des garanties appropriées afin d'assurer la confidentialité des données médicales personnelles, et de limiter et soumettre à certaines conditions leur utilisation et leur divulgation sans le consentement du patient. La règle accorde également aux patients un droit de regard sur leurs données médicales : ils peuvent notamment consulter leur dossier médical et demander une reprographie ou des rectifications. L'*American Recovery and Reinvestment Act* (ARRA) (plan de relance économique) et le Health Information Technology for Economic and Clinical Health Act (HITECH) (loi relative à l'utilisation des technologies de l'information dans le domaine de la santé) encouragent, avec force mesures incitatives, l'utilisation à grande échelle des dossiers de santé électroniques (DSE). Ils contiennent également des dispositions relatives à la protection des données, notamment les mesures prévues en cas de violation de la sécurité et de la confidentialité des données (États-Unis, 2009).

18. L'Union africaine (UA) et la Coopération économique Asie-Pacifique (CEAP) sont d'autres exemples d'organisations régionales ayant établi des cadres juridiques régionaux pour la protection des données personnelles et de la vie privée. La Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel prévoit que « les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé » doivent être « mis en œuvre après autorisation de l'autorité nationale de protection » (UA, 2014, article 10, paragraphe 4, point a). Le cadre actualisé de protection de la vie privée de la CEAP (*APEC Privacy Framework*) prévoit la mise en place d'un « mécanisme multilatéral permettant aux instances de la CEAP chargées de la protection de la vie privée de s'entendre sur l'application transfrontalière des lois sur la protection de la vie privée » (CEAP, 2015).

19. Concernant la protection des données, de l'autonomie et de la vie privée, la notion juridique de propriété est également importante. Il est essentiel de bien distinguer découverte et invention. Les inventions peuvent normalement faire l'objet de brevets, de par leur activité inventive et leur utilisation à l'échelle industrielle. Le 3 juillet 2012, la Cour de justice

européenne a publié un arrêt majeur dans le cadre de l'affaire C-128/11 opposant UsedSoft GmbH et Oracle International Corp. L'arrêt implique que les biens incorporels, tels que les logiciels téléchargés à partir d'Internet, sont soumis à des droits de propriété spécifiques. Bien que l'applicabilité de ce modèle à d'autres biens numériques n'ait encore fait l'objet d'aucune autre décision judiciaire, l'arrêt C-128/11 a ouvert le débat sur la propriété des biens incorporels (Hoeren, 2014). Par ailleurs, dans l'appel interjeté contre la décision rendue dans l'affaire opposant Football Dataco Ltd. et Brittens Pools Ltd. en avril 2010, la Cour de justice européenne précise que la directive 96/9/CE sur la protection juridique des bases de données a pour finalité de « stimuler la mise en place de systèmes de stockage et de traitement de données afin de contribuer au développement du marché de l'information (…) et non de protéger la création d'éléments susceptibles d'être rassemblés dans une base de données » (paragraphe 34).

20. À l'échelle internationale, l'article 10, paragraphe 2 de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) dispose que « [l]es compilations de données ou d'autres éléments, qu'elles soient reproduites sur support exploitable par machine ou sous toute autre forme (…) seront protégées (…) » à condition que « par le choix ou la disposition des matières [elles] constituent des créations intellectuelles » (Organisation mondiale du commerce [OMC], 1994). L'article précise le champ d'application des droits relatifs auxdites compilations et dispose que « [c]ette protection, qui ne s'étendra pas aux données ou éléments eux-mêmes, sera sans préjudice de tout droit d'auteur subsistant pour les données ou éléments eux-mêmes » (OMC, 1994).

21. Le Conseil de l'Union européenne a pris des mesures importantes quant à la protection juridique des bases de données (UE, 1995 ; UE, 1996, article 7, paragraphe 4). Ainsi, des dispositions spécifiques et distinctes s'appliquent pendant 15 ans ; chaque modification substantielle de la base de données lui confère cependant une durée de protection propre. Le propriétaire de la base de données est en droit de contester la reproduction de parties substantielles de sa base de données, quand bien même les données seraient extraites et rassemblées une par une. L'agencement, la sélection et la présentation des données peuvent bénéficier de la protection juridique du droit d'auteur, tandis que la législation relative aux bases de données peut protéger l'intégralité d'une base de données.

III. VISIONS, TENDANCES ET DÉFIS

22. Les mégadonnées dans le domaine de la santé peuvent se concevoir comme une médecine globale et personnalisée sur la base de preuves, une médecine appelée médecine de précision sur la base de stratification de populations, une médecine qui combine les meilleures connaissances scientifiques disponibles avec l'expérience professionnelle des professionnels de santé au bénéfice du patient indivudel. Cette approche est le fruit des avancées technologiques réalisées dans la génomique et les autres technologies « omiques » ou technologies à très hauts débits, grâce auxquelles l'analyse moléculaire des échantillons humains est devenue considérablement moins coûteuse et plus efficace. Les données moléculaires peuvent être complétées par des clichés d'imagerie médicale numérisés (à l'échelle microscopique ou du corps entier) et des données sur l'environnement et le mode de vie recueillies auprès de diverses sources (enquêtes, groupes tels que populations, cohortes de patients, etc., infrastructures de recherche, registres et bases de données). Les données recueillies peuvent également couvrir l'environnement social, la communication et le comportement. Elles autorisent une compréhension beaucoup plus fine de la santé et des maladies, selon le modèle biopsychosocial avancé par l'OMS. Selon cette approche, toutes ces données associées à celles des DSE devraient à l'avenir révolutionner les méthodes actuelles et permettront de personnaliser le diagnostic et la prise en charge, en fournissant aux patients des conseils pertinents et un traitement personnalisé au bon moment. Elle permettra en outre de favoriser la sécurité des patients, en combinant les différentes données provenant de diverses sources afin d'analyser et finalement de prévenir des situations indésirables.

23. Par ailleurs, les connaissances de plus en plus pointues des individus nous permettront petit à petit de déterminer les prédispositions à certaines maladies de chaque individu et son profil de risque, et ainsi, de lui fournir des conseils de prévention ciblés en temps voulu.

24. Il est également probable qu'à l'avenir, la collecte des données sur la santé aux fins de diagnostic, de suivi et de traitement soit réalisée à distance. Les données pourront alors être utilisées à des fins de dépistage précoce de maladies, comme les risques imminents d'infarctus, et permettront ainsi la formulation de recommandations sur le comportement à adopter. Elles contribueront également à fiabiliser la télémédecine dans les régions isolées, ce qui peut renforcer l'accès à des soins de qualité et ainsi contribuer à améliorer la santé dans le monde.

25. Les patients pourront plus facilement accéder à leurs données personnelles et exercer un droit de regard. Par exemple, ils pourront consulter leur DSE directement sur leur téléphone portable. Les smartphones devraient jouer un rôle essentiel dans l'autocoordination des soins de santé et la création de réseaux de santé personnels, en encourageant ainsi l'acquisition d'une autonomie accrue et de meilleures connaissances sur la santé.

26. S'ils disposent d'un meilleur accès aux informations médicales ainsi qu'au profilage individualisé et aux recommandations (dont la qualité aura été avérée), les citoyens seront mieux informés de leur état de santé et des comportements à adopter pour une meilleure hygiène de vie et pourront faire bon usage de ces informations. Toutefois, cela ne sera possible que si les personnes prennent des mesures concrètes pour améliorer leur santé, ce qui n'est souvent pas le cas, même lorsqu'elles sont conscientes des risques. Un exemple frappant est celui du tabagisme.

27. Les applications mobiles de santé jouent un rôle croissant dans les soins de santé et la recherche. De grandes avancées sont attendues dans plusieurs domaines, par exemple le suivi de mesures sanitaires, l'évolution positive des comportements en matière de santé et l'aide au diagnostic. Toutefois, la qualité de ces applications n'est pas encore officiellement évaluée et surveillée et il n'existe guère de cadre réglementaire ou de système sérieux de vigilance. La fréquence des mises à jour représente un autre obstacle à l'évaluation adéquate des applications mobiles de santé.

28. Dans ce contexte, au moins quatre changements de paradigme dans le domaine de la santé individuelle sont susceptibles de se produire: le passage d'une orientation sur la maladie vers une orientation sur la santé ; d'un focus sur la thérapie vers un focus sur la prévention ; de conseils de santé à des conseils de mode de vie ; du rôle de patient à un rôle d'utilisateur, de client ou de « citoyen numérique ».

29. Les mégadonnées permettraient également à l'industrie pharmaceutique de mieux connaître les maladies et leurs mécanismes sous-jacents, et ainsi de mettre au point des médicaments, dispositifs et traitements mieux ciblés. Elles devraient en outre permettre de concevoir des études cliniques stratifiées et ainsi réduire le nombre de participants et les coûts, et obtenir des résultats plus rapidement.

30. Ces perspectives sur les mégadonnées ne concernent pas uniquement la santé individuelle et la recherche médicale. Ces nouvelles données devraient également contribuer à étayer les politiques de santé publique, notamment en améliorant les stratégies de prévention axées sur les risques à destination des différents groupes ciblés.

31. Les organismes de réglementation seraient mieux à même de comprendre et de maîtriser le processus de conception des études. Leurs politiques pourraient tirer parti d'uneaméliorations de la pharmacovigilance. Lorsqu'un nouveau médicament pénètrera sur le marché, les mégadonnées permettront de recueillir et d'analyser les données en vie réelle de très nombreux patients, sur une longue période. La majorité de la population mondiale vit dans des zones desservies par les réseaux de téléphonie mobile, ce qui renforcera nécessairement la participation des citoyens à la production et à l'apport de données.

32. Par ailleurs, les mégadonnées peuvent contribuer à soutenir des systèmes de santé en apprentissage (Organisation internationale pour les migrations [OIM], 2007 ; OIM, 2013). Les expériences quotidiennes peuvent renseigner sur les meilleures et les plus efficaces manière de gérer les diagnostics, les mesures thérapeutiques et préventives, et de façonner les structures au service des systèmes de santé et de la recherche. Elles permettent d'analyser des données de la vie réelle sur la santé de façon structurée et avec un contrôle de qualité. Citons, par exemple, le travail de l'OCDE : sur les systèmes de santé en apprentissage, les projets européens tels que CORBEL (Coordinated Research Infrastructures Building Enduring Life-science Services, http://www.corbel-project.eu/about-corbel.html), et des outils pratiques facilitant le partage des données, comme IMI 2014 (Initiative en matière de médicaments innovants), ainsi que des initiatives dans l'industrie (OCDE, 2013b ; OCDE, 2015 ; CORBEL ; IMI, 2014 ; PhRMA, 2014). L'Agence européenne des médicaments (EMA) a récemment publié des directives sur la publication des données individuelles anonymisées des patients lors des essais cliniques (EMA, 2016).

33. Gardant à l'esprit la vaste définition de la santé retenue par l'OMS, et reconnaissant le fait que, la majeure partie de l'état de santé d'un individu ne dépend pas uniquement des prestations de santé, mais également de déterminants sociaux, comprenant, entre autres, les inégalités sociales, l'éducation, le mode de vie et l'environnement, les mégadonnées ouvrent la voie à une vision holistique de la santé, en regroupant différents types de données (ex : à partir de registres, d'applications et d'archives médicales).

34. Ces visions et ces tendances s'accompagnent de grands défis technologiques, mais aussi de défis d'ordre éthique, social et juridique (voir chapitre IV).

35. La possibilité d'adopter une vision globale de la santé estompe également davantage la frontière entre le secteur de la santé et les autres domaines sociétaux. Aux sources traditionnelles de données sur la santé, telles que les dossiers médicaux ou les résultats d'analyses biologiques, s'ajoutent désormais des sources extérieures, par exemple les réseaux sociaux, les données sur la consommation ou celles provenant d'organismes publics non liés à la santé (Trésor public, ministère de l'Éducation, ministère des Services sociaux). Les fournisseurs de moteurs de recherche collectent aussi systématiquement de nombreuses données sur leurs utilisateurs, celles-ci étant ensuite traitées et vendues à d'autres entreprises, qui s'en servent pour créer des « stratégies marketing ciblées » et proposer aux internautes des contenus publicitaires personnalisés, en fonction de leur historique de recherche ou de leur participation à certains forums en ligne, par exemple. Ce « profilage client » n'épargne pas le secteur de la santé — une simple recherche « privée » effectuée sur Internet pour se renseigner sur telle ou telle maladie (pour soi ou sa famille) devenant une information échappant à la sphère strictement privée à l'insu de la personne. Il ne fait donc aucun doute que la protection, la confidentialité ainsi que la qualité des données sont autant des défis compexes.

36. Les méthodes prédictives d'apprentissage automatique s'avèrent très productives en médecine. Toutefois, il est essentiel de bien comprendre les hypothèses sous-jacentes et de veiller à ce que les conditions, telles que la stabilité (c'est-à-dire que les circonstances dans lesquelles les données ont été collectées demeurent inchangées), soient réunies afin de garantir la qualité des données, ainsi que la validité et l'utilité des conclusions. Les mégadonnées permettent principalement de créer des modèles et d'établir des corrélations. Une mauvaise compéhension des liens de causalité pourrait entraîner des conséquences fâcheuses et préjudiciables.

37. En outre, les algorithmes de reconnaissance de structures et ceux utilisés dans les applications mobiles de santé peuvent être d'emblée biaisés ou être difficilement compris et contrôlés sur le plan de la transparence technique.

38. Un des problèmes est la possible inexactitude et imprécision lors de la collecte et de la classification des données en raison de leur énorme quantité, de leur hétérogénéité, de leur accumulation rapide, de la gestion rapide, et des différents contextes de données. Il peut y

avoir des erreurs dans le processus de collecte des données par le patient/ citoyen, par le professionnel de la santé (ex : enregistrement incomplet, classification inadéquate, analyse imprécise) ou par la technologie (bio)informatique (dû par exemple à des algorithmes biaisés ou imprécis, ou un manque d'intéraction entre cliniciens et informaticiens). Les inexactitudes et erreurs dans la collecte et l'analyse peuvent avoir des conséquences négatives à la fois pour le patient/citoyen individuel et pour la société (CE, 2015).

39. En conséquence, l'ensemble des acteurs impliqués devront posséder les compétences et les savoir-faire requis. Les professionnels de la santé devront être en mesure de comprendre, vérifier et utiliser correctement les données disponibles. Les chercheurs, les citoyens et les décideurs devront comprendre l'importance des différents contextes des données et les implications des algorithmes. Les données et leurs contextes doivent pour cela être transparents et compréhensibles. Cela n'est possible que si les algorithmes sont accessibles et s'il existe des modèles expérimentaux et des politiques visant l'affectation optimale des ressources.

40. On assistera également au décloisonnement des différentes professions. Certaines maladies ne seront plus envisagées à l'échelle de l'organe atteint, mais à l'aune des mécanismes moléculaires sous-jacents, des types de mutation et des variantes révélés par les disciplines dites « omiques ». Afin d'optimiser la prise en charge de chaque patient et la recherche, les systèmes de santé doivent privilégier une approche pluridisciplinaire, comme celle déjà appliquée par de nombreux pays dans la lutte contre le cancer. Celle-ci peut également contribuer à l'émergence de nouvelles disciplines. Par ailleurs, l'intégration de disciplines comme les sciences sociales, l'économie comportementale, l'épidémiologie, etc. pour permettre une compréhension globale de la santé et une bonne utilisation des données dans les méthodes d'inférence causale.

41. Les développements en mégadonnées offrent des nombreuses opportunités d'amélioration de la santé et pourraient signifier une économie d'argent permettant de préserver des systèmes de santé et les rendre durables. Néanmoins, ces développements technologiques présentent également des défis pour les professionnels de la santé. La mise en œuvre de nombreuses procédures technologiques peut réduire le nombre d'au moins certains types de professionnels de la santé dont le système de santé a besoin, ils auront probablement besoin de différentes compétences, et cela pourrait causer un fossé entre les différentes générations de professionnels de la santé. Ainsi, il est crucial d'adapter le système d'éducation à ce nouveau contexte et d'améliorer la formation continue des professionnels de la santé.

42. Finalement, le flux de mégadonnées et la multiplication des capteurs individuels rend les individus de plus en plus transparents, mais paradoxalement accentue l'opacité de l'environnement technologique, des algorithmes, des retombées de l'analyse des données et de la pondération sous-jacente des facteurs. Cela pose de réels problèmes d'ordre éthique, notamment à l'égard de l'autonomie, de la vie privée et de la justice (voir chapitre IV).

43. Dans de nombreux pays, plus particulièrement ceux en développement, les infrastructures éthiques et scientifiques au service de la recherche ne sont pas tout à fait au point et beaucoup sont encore loin de tirer pleinement profit des bienfaits potentiels de l'utilisation des mégadonnées. L'accès aux données reste problématique et les plateformes d'information sanitaire en mesure de stocker de grands volumes de données et de traduire les informations existantes en actions concrètes demeurent insuffisantes. Le renforcement des capacités est indispensable. En effet, il constitue un moyen judicieux de garantir que la participation des scientifiques et des professionnels de la santé des pays en développement aux projets de coopération internationaux ne se résume pas au recueil de données, mais contribue activement à la transformation des données en bienfaits tangibles dans le domaine de la santé pour leurs propres citoyens.

44. Par ailleurs, les recherches de pointe menées en médecine de précision sont coûteuses et restent l'apanage des pays riches ; les approches en matière de mégadonnées

n'incluent pas encore de manière adéquate les maladies présentes dans les pays où les infrastructures sanitaires sont moins avancées. Il est nécessaire de moderniser le traitement des données des systèmes de santé actuels avant de mettre en place une médecine de précision axée sur les mégadonnées. Les mégadonnées pourront alors permettre d'améliorer les interventions médicales et les services de santé, mais aussi les stratégies de prévision et de prévention, ainsi que les politiques de santé en général.

45. Il est très difficile de prévoir la vitesse et l'ampleur avec lesquelles les tendances décrites ci-dessus se généraliseront. Si la théorie se veut optimiste, la prudence reste toutefois de mise. Il s'agit de ne pas surestimer l'état des connaissances scientifiques actuelles ni les avantages potentiels des mégadonnées et de la médecine de précision pour les systèmes de santé dans le monde. L'enthousiasme suscité par le phénomène des mégadonnées risque d'entraîner des suréstimations et des prévisions irréalistes, ainsi que de commercialisation de produits et de services n'ayant pas encore fait la preuve de leur pertinence. En outre, cela peut mener à un déséquilibre des priorités en termes de politiques de santé ce qui peut avoir des effets particulièrement nocifs pour les pays où l'accès aux services essentiels n'est pas garanti. Cependant, il serait tout aussi risqué de négliger le potentiel bénéfique des mégadonnées et de ne pas mettre à profit leurs avantages. Il est par conséquent essentiel de gérer avec bon sens l'optimisme suscité par ce phénomène.

IV. ASPECTS ÉTHIQUES

IV.1. Autonomie et consentement

46. L'autonomie dont jouit l'individu dans l'exercice de son autodétermination comporte sept dimensions (Mertz *et al.*, 2016):

a. L'individu a les *capacités* d'accéder à l'information, de la comprendre, de l'évaluer et de la mettre en pratique.

b. Il dispose d'*informations* sur le sujet, à la fois compréhensibles et pertinentes.

c. Il a le *choix* entre plusieurs solutions (agir ou s'abstenir, ou choisir entre plusieurs possibilités).

d. Ses *valeurs*, ses préférences et ses attitudes sont prises en compte dans la décision et l'acte.

e. Il peut prendre des décisions et *agir de son propre chef* sans aucune contrainte extérieure ou intérieure.

f. Il peut choisir un but et le moyen le plus approprié pour l'atteindre (*formation de la volonté*).

g. L'*action* désigne un acte conscient ou un refus conscient d'agir.

47. Le consentement est la principale garantie généralement appliquée afin de protéger l'autonomie des êtres humains dans le cadre de la médecine et de la recherche. Les articles 5, 6 et 7 de la Déclaration universelle sur la bioéthique et les droits de l'Homme sont consacrés à l'autonomie, à la responsabilité individuelle, au consentement, ainsi qu'à la protection des personnes incapables d'exprimer leur consentement. L'article 6, paragraphe 1 de ladite Déclaration dispose que les interventions médicales de caractère préventif, diagnostique ou thérapeutique, ainsi que la recherche scientifique, ne doivent « être mise[s] en œuvre qu'avec le consentement préalable, libre et éclairé de la personne concernée » (UNESCO, 2005). Le *Code de Nuremberg,* qui s'intéresse au consentement, est à l'origine du concept selon lequel la participation à une recherche est une activité volontaire. La *Déclaration d'Helsinki* désigne également le consentement comme principale garantie.

48. Le contrôle et la prise de décisions avisées quant aux utilisations qui sont faites des données personnelles sont devenus quasiment impossibles, en raison de l'ampleur et de la complexité du traitement auquel sont soumises les données personnelles dans le domaine des mégadonnées. Les sept dimensions mentionnées ci-dessus posent de grandes difficultés.

Même en supposant que les individus puissent contrôler leurs données et s'informer de leur(s) utilisation(s), leurs choix risqueraient d'être faussés en raison des difficultés liées au processus décisionnel. Cela se traduit par une perte d'autonomie et donc, de contrôle et de liberté sur les décisions prises dans des environnements technologiques et dans le cadre de processus automatisés. La gouvernance devra veiller à compenser ce manque, en garantissant que toutes les dimensions relatives à l'autonomie sont respectées et appuyées (voir chapitre V).

49. Un problème ultérieur du consentement obtenu de manière électronique (« consentement électronique ») est qu'il ne permet pas de connaître l'âge de l'utilisateur et d'adapter les contenus en fonction de son âge et de ses capacités de compréhension (CE, 2012). L'éducation des mineurs en tant qu'utilisateurs actifs de ces nouvelles technologies, constitue notamment une priorité importante.

50. La notion de consentement est généralement plus spécifique dans le cadre des essais cliniques, car elle s'inscrit dans un projet de recherche donné. Bien souvent, cela exclut l'utilisation des échantillons ou des données en dehors du cadre des recherches originales ou primaires pour lesquelles les participants ont spécifiquement donné leur consentement. Pour que le consentement soit libre et éclairé – et donc valable –, les participants doivent recevoir au préalable les informations nécessaires et comprendre la nature, les risques et les éventuels avantages du programme.

51. Il est impossible de prédire quelle sera l'utilisation secondaire potentielle des mégadonnées obtenues à partir des vastes bases de données, telles que les biobanques, et encore moins dans le domaine de la recherche faisant appel aux mégadonnées, d'autant qu'elles impliquent des interrelations entre des sources de données nombreuses et variées, médicales et non médicales. Certains ont donc exigé la création d'un modèle de consentement plus adapté, qui permette une large utilisation des données dans le respect de l'autonomie du participant ou du patient. Le secteur des biobanques a déjà fait de nouvelles propositions sur l'obtention d'un *consentement global*.

52. Le consentement global peut inclure des activités très diverses ou se limiter à certaines utilisations sans que celles-ci soient vraiment spécifiées, comme la recherche des causes de maladies complexes. Le consentement global ne s'oppose donc pas au consentement « spécifique » dans la mesure où, selon le CIB, il ne s'agit pas d'un consentement général ou ouvert, qui n'est rattaché à aucune condition même s'il est généralement plus abstrait. Le consentement global se réfère au même modèle de consentement éclairé, toutefois le patient ou le participant accepte que ses données soient utilisées dans le cadre des *différents projets* de recherche susceptibles d'être menés dans une branche ou un domaine particulier. Pour qu'il soit valable, le consentement global requiert une certaine forme de gouvernance et de garantie, assurée, par exemple, par un comité compétent qui examine les propositions afin de veiller à ce que les droits et les intérêts des individus soient dûment protégés ou que les garanties prévues par la loi soient respectées.

53. Cette approche de consentement éclairéglobal, utilisée en Europe, est de plus en plus reconnue (Association médicale mondiale [AMM], Conseil des organisations internationales des sciences médicales [CIOMS]). En donnant son consentement global, le sujet autorise toute forme de recherche sur ses échantillons biologiques dans une branche ou un domaine particulier. Ce modèle suscite également un intérêt croissant dans les pays en développement, par exemple dans le domaine de la génomique et des biobanques, mais il existe des préoccupations suite à de mauvaises expériences dans le domaine des biobanques. Avec des garanties suffisantes, comme des contrôles garantissant que les données ne serviront pas à prendre une décision concernant la personne ou ne seront pas utilisées de sorte que la personne et/ou la communauté s'en trouvent affectées, le recours au consentement global convient à des fins de recherche contribuant à l'intérêt public.

54. Une autre approche est celle du consentement présumé : les données médicales du sujet peuvent être utilisées aux fins de recherche sauf en cas de refus exprès de l'intéressé.

Le sujet doit être correctement informé au préalable, notamment des conséquences éventuelles liées à la collecte d'échantillons biologiques et de données personnelles. Ainsi, les prestataires doivent communiquer certaines informations et connaissances, mais manquent souvent de temps. La situation hors du cadre de la recherche est tout autre. Il est quasiment impossible d'être radié des bases de données commerciales liées à la santé (opérateurs de téléphonie mobile, fournisseurs Internet, applications, bases de données commerciales, bases de données relatives au comportement des consommateurs) ; une situation particulièrement inquiétante sachant que ces bases de données ne font l'objet d'aucun contrôle, ou presque.

55. Conformément aux principes de participation et de transparence, un nouveau modèle de consentement qui dépend de la disponibilité et de l'accessibilité aux TIC a été proposé : le « consentement dynamique ». Là encore, le sujet donne son consentement initial, mais il est tenu informé de l'utilisation qui est faite de ses données et peut choisir de refuser ou d'autoriser certaines utilisations. Les pouvoirs publics doivent garantir le respect des droits individuels et encourager la participation des citoyens par le biais de campagnes d'éducation et d'information. Cette approche favorise l'autonomisation, les sujets et les patients pouvant surveiller l'utilisation qui est faite de leurs données médicales. Dans certains cas, ils peuvent contrôler eux-mêmes l'accès à leurs données par le biais de mécanismes tels que des portails dédiés. Les apports continus des participants et leurs choix en matière d'utilisation des données (en donnant leur permission, c'est-à-dire en « votant » pour les utilisations auxquelles ils consentent) leur permettent d'influer sur les possibilités de la recherche et de devenir ainsi de véritables parties prenantes. Le patient participe activement au projet qui devient alors une entreprise collective ou partagée entre les patients et les chercheurs, éliminant ainsi les risques d'exploitation ou d'utilisation abusive de la personne (Conseil de Nuffield, 2015). Ce modèle pourrait s'avérer efficace dans les pays développés bénéficiant de technologies de pointe permettant aux patients de surveiller l'utilisation de leurs données via une base de données et aux personnes prêtes à consacrer le temps et la volonté nécessaires pour suivre l'utilisation de leurs données. Cependant, il sera plus difficile à mettre en place dans les zones moins développées, en raison, entre autres, du manque de technologies locales et du faible taux d'alphabétisation, de la nécessité de se consacrer à d'autres activités ou de l'absence de sensibilisation et d'éducation du public qui pourraient donc limiter la compréhension des patients en matière de soins et de participation aux recherches.

56. Le consentement pose un réel problème en ce qui concerne les applications mobiles de santé et les réseaux sociaux. Les informations communiquées au format numérique sont généralement affichées en petits caractères pour s'adapter aux écrans des téléphones portables, et ne fournissent parfois aucune possibilité de désabonnement. L'utilisateur doit donner son consentement éclairé sur un écran (et non sur papier) sans avoir accès à aucun conseil pour le guider dans son choix. Généralement, il clique rapidement sans prendre le temps de réfléchir et sans réelle prise de conscience, compétence ou intention. Les conditions de vente, généralement longues et incompréhensibles pour la plupart des gens, sont rarement lues. Il est alors peu probable que cette formule d'« accepter tout en un seul clic » constitue vraiment un consentement donné d'une manière libre et éclairée. Mener des recherches et des enquêtes sur la santé par des moyens électroniques peut néanmoins s'avérer efficace et performant tant que des garanties existent pour assurer l'autonomie des participants.

57. Compte tenu de la difficulté d'obtenir un consentement autonome concernant la collecte et l'utilisation de mégadonnées et des limites des modèles de consentement proposés, il est important que l'éducation publique contribue à l'acquisition de cette autonomie afin que les utilisateurs, les patients et les participants aux recherches soient en mesure de comprendre la portée et l'impact de l'utilisation de leurs données.

58. Bien qu'il faille insister sur le fait que le respect de l'autonomie touche directement au respect de la dignité humaine, la recherche dans le secteur des mégadonnées et de la santé pourrait s'avérer très profitable pour la collectivité, en ce sens qu'elle contribue à l'instauration d'une médecine de précision reposant sur des données d'observation objectives et

nombreuses, ainsi qu'à l'apprentissage croisé dans les systèmes de santé. L'enjeu consiste donc à trouver un juste équilibre entre intérêt individuel et intérêt collectif. Il peut alors être envisagé de lancer un appel à la solidarité pour que chacun consente à participer à la recherche médicale fondée sur ses données en partageant les informations qui le concernent de façon anonyme (et non personnelle), et alimente ainsi de grandes bases de données. Le principe de réciprocité solidaire laisse supposer qu'une personne bénéficiant des résultats d'une recherche médicale souhaite que d'autres profitent aussi des avancées de la recherche, à condition qu'il soit possible de garantir que le résultat sera bénéfique et constituera un bien public, tel que défini démocratiquement, et que l'utilisation abusive ou la désanonymisation non légitime des données feront l'objet de poursuites judiciaires et seront fermement condamnées. Dans un tel contexte, au moins deux éléments sont essentiels à prendre en compte pour garantir l'équilibre entre intérêt individuel et intérêt collectif : la vulnérabilité des personnes dont les données sont collectées et la finalité de l'utilisation des données.

59. Dans le cas où la recherche envisagée s'inscrit hors du champ du consentement global qui a été obtenu pour l'utilisation de ces données, un consentement spécifique est nécessaire pour le traitement des données secondaires. C'est un principe essentiel pour garantir la confidentialité et le caractère privé des données. Néanmoins, l'analyse secondaire des données pourrait être éthiquement acceptable sans nouveau consentement informé pour un tel usage secondaire si les exigences suivantes sont remplies:

a. fondement juridique approprié ;
b. évaluation par le comité d'éthique de la recherche (CER) ;
c. procedures techniques adéquates pour empêcher les chercheurs et les tiers d'accéder aux données personnelles, tells que la pseudo-anonymisation ;
d. intérêt public supérieur dans cette recherche ;
e. impossible d'obtenir un nouveau consentement ;
f. les données doivent avoir été collectées selon les exigences éthiques et légales.

IV.2. Confidentialité et respect de la vie privée

60. Selon l'article 9 de la Déclaration universelle sur la bioéthique et les droits de l'Homme, « [l]a vie privée des personnes concernées et la confidentialité des informations les touchant personnellement devraient être respectées » (UNESCO, 2005). « [C]es informations ne devraient pas être utilisées ou diffusées à des fins autres que celles pour lesquelles elles ont été collectées ou pour lesquelles un consentement a été donné ». Les mégadonnées risquent de compromettre la protection de la vie privée et de la confidentialité des données, et ce, pour plusieurs raisons.

61. Les principes traditionnels de protection des données, tels que la limitation de la finalité, la rareté et la minimisation des données, la protection spéciale des données sensibles, le traitement loyal et la protection des droits des personnes concernées, ont été largement mis en œuvre aux fins de protection de la vie privée, bien que les systèmes de protection et les notions sous-jacentes diffèrent d'une région du monde à l'autre. En revanche, les mégadonnées impliquent un changement et un élargissement de la finalité, une masse infinie de données, un traitement opaque, un faible niveau de protection des données (l'objectif étant d'accéder à un maximum de connaissances) et une absence de transparence à l'endroit des personnes concernées. Cela est particulièrement vrai à l'heure de l'intelligence artificielle et de l'apprentissage en profondeur, et des algorithmes qui sont de plus en plus complexes et indéchiffrables.

62. En outre, l'anonymisation des données personnelles ne suffit plus à protéger la vie privée et la confidentialité dans certaines circonstances, et en fonction de l'assessibilité à d'autres sources de données. En effet, il pourrait être désormais possible de retrouver l'identité des personnes concernées en intégrant simplement les masses de données provenant de différentes sources. Les garanties réduisant le risque de réidentification sont

essentielles pour que l'anonymisation reste un outil efficace de protection des personnes tout en offrant la possibilité d'utiliser les mégadonnées dans l'intérêt public.

63. Le profilage différencié est une pratique de plus en plus répandue, qui permet de cibler et d'influencer des groupes selon certains profils spécifiques (on parle d'« identités de groupe »). L'anonymat ne suffit plus à protéger la vie privée des personnes, qui peuvent être identifiées grâce à l'adresse IP de leur ordinateur ou de leur téléphone portable, par exemple. La « vie privée des groupes » est par conséquent une notion dont il faut de plus en plus tenir compte dans l'utilisation des mégadonnées. L'Assemblée parlementaire du Conseil de l'Europe a même proposé de reconnaître un nouveau droit : celui de toute personne concernée à ne pas faire l'objet de mesures de profilage (Rathenau Instituut, 2017).

64. Ce nouveau droit donnerait acte qu'avec l'arrivée des mégadonnées, la vie privée en tant que concept ne se limite pas à la seule protection des données individuelles. La collecte, le stockage, le traitement, l'analyse et l'application des données de manière indéfinie (ce que l'on appelle le cycle de la cybernétique) impliquent également l'intrusion dans la sphère privée de contenus ciblés (informations principalement à but commercial, offres, publicités, etc.), diffusés sur les écrans des objets électroniques. Ces contenus sont adaptés au profil de l'utilisateur et élaborés par des algorithmes obscurs à partir de données recueillies auprès de diverses sources. Cette ingérence touche plusieurs aspects de la vie privée, tels que les communications d'ordre personnel, le lieu, et la participation à des associations ou des groupes. Dans ce contexte, le droit de ne pas être l'objet de mesures de profilage est d'autant plus important.

65. Le droit au respect de la vie privée est étroitement lié au droit à la liberté, lequel comprend plusieurs aspects juridiques et éthiques : liberté d'expression, d'association, de mouvement et d'espace, de croyance, de pensée et de sentiment, et de comportement. Dans le présent contexte, le CIB utilise le terme « vie privée » dans la suite du texte comme le droit au respect de la vie privée et s'applique aux domaines de la vie ou aux données que les individus ne souhaitent pas divulguer, ou alors uniquement à certains membres de leur famille ou à certaines relations.

66. Si les individus ont intérêt à protéger leur vie privée, ils trouvent également un intérêt général dans l'utilisation de leurs données aux fins de recherche médicale. L'intérêt général et la vie privée des individus sont parfois en conflit, toutefois, leur relation ne se réduit pas à cette opposition. Ils sont inextricablement liés : les individus peuvent trouver leur compte dans certains projets collectifs, et la protection de la vie privée peut trouver un écho dans la sphère publique, ce qui favorise la coopération. Au vu de ces liens complexes, il est nécessaire de faire converger l'intérêt général et l'intérêt particulier.

67. Comme en témoignent plusieurs enquêtes, les individus sont conscients du fait qu'ils n'ont quasiment aucune maîtrise de la collecte et de l'exploitation de leurs données personnelles, bien que la majorité d'entre eux veuille exercer un certain contrôle en la matière. À long terme, cette situation est susceptible entraîner une méfiance, qui pourrait sérieusement compromettre les efforts et projets essentiels de promotion de la santé publique à l'avenir. Il est impératif d'améliorer la confiance de la population afin de protéger mieux la vie privée et l'intérêt général : les individus doivent être assurés que leurs données médicales sont utilisées à bon escient et protégées. Des mécanismes devront être mis en place à plusieurs niveaux : législation, gouvernance, vigilance citoyenne, conception d'applications et d'appareils respectueux de la vie privée, et respect de la vie privée par défaut, par example au regard des prérequis de consentement préinstallés

68. Afin de protéger la vie privée au sens large décrit ici, de nouveaux modèles doivent être appliqués concernant la participation à la collecte et à l'exploitation des données (voir chapitre sur l'autonomie), la sensibilisation et l'information du public sur les incidences de l'utilisation des mégadonnées, la gestion efficace de la protection des données, la redevabilité auprès des participants et de la société en général. Cette question requiert également

l'élaboration de modèles innovants de propriété et de tutelle des données au sens large détaillé ici.

IV.3. De la propriété à la conservation et au partage des bienfaits

69. La propriété des données personnelles et les droits associés — notamment la restriction de l'accès à des tiers — doivent être conférés, sans l'ombre d'un doute, à la personne ou au groupe auprès desquels ont été recueillies les données. De la propriété, découle le droit des personnes à suivre et à contrôler l'existence et le traitement de leurs données. Le fait d'avoir le contrôle sur ce que nous sommes, de nos actessur ce que nous faisons, sur ce que nous pensons, et sur ce que nous portons à la connaissance des autres et de la société en ce qui concerne nos données personnelles représente un aspect essentiel de la liberté au XXIe siècle (voir aussi chapitre IV.2.).

70. Comme pour les autres domaines de la biomédecine, il est important de distinguer deux notions de propriété en matière de mégadonnées : la propriété des données et la propriété des résultats opérationnels. Dans le premier cas, la propriété est un mécanisme servant à contrôler les données ; dans le second, la propriété se rapporte aux produits tels que les algorithmes, médicaments, outils de suivi, etc. et à la propriété intellectuelle.

71. Il est posé comme principe que les bénéfices liés à l'exploitation des données résulteront d'un partage équitable avec l'ensemble de la communauté scientifique, ce qui favoriserait les découvertes scientifiques. Il existe aussi un nombre croissant d'études académiques sur les cadres éthiques pertinents qui devraient guider les bonnes pratiques en matière de partage de données dans le cadre des partenariats de recherche internationaux. Cela inclut l'utilisation de méthodes délibératives en vue de consulter l'avis des parties prenantes clés. Il semblerait qu'il existe un consensus croissant dans la communauté scientifique sur l'importance d'un partage plus large des données de recherche. En même temps, il y a de serieuses inquiétudes au sujet du partage de données, incluant le consentement, la propriété des données, les droits de propriété intellectuelle qui s'y rattachent et les questions de confidentialité.

72. Dans ce contexte il est de plus en plus problématique, et parfois impossible, de résoudre les problèmes juridiques et éthiques avec les concepts associés à la notion de propriété, notamment lorsqu'il s'agit d'analyse en temps réel, de corrélation et de partage de grandes bases de données, ainsi que de l'utilisation des bases de données à différentes fins par le milieu médical et celui de la recherche, simultanément ou non. Pour des questions liées aux moyens techniques, aux compétences et aux ressources financières, peu d'entreprises et d'institutions sont en mesure de gérer de très grandes bases de données, ce qui exclue d'autres de la capacité d'acquérir des connaissances et de développer des outils en faveur de la santé de tous. Par conséquent, les notions de propriété semblent ne plus fournir un cadre normatif approprié, en particulier au regard de ce qu'on appelle la fracture numérique. Le phénomène des mégadonnées signale plutôt la nécessité de developer un cadre normatif alternatif qui comprenne de nouveaux concepts pour trouver l'équilibre entre les intérêts légitimes et les bénéfices.

73. Le nouveau contexte créé par les mégadonnées peut être considéré comme une occasion de revoir notre vision traditionnelle et d'élaborer de nouveaux moyens éthiques et juridiques pour un véritable schéma de partage des bénéfices. Il est nécessaire de concilier les droits et les intérêts de tous les acteurs concernés : l'individu duquel proviennent les données, les chercheurs, les entreprises et les organisations utilisant les données, et la société en général, puisqu'elle peut bénéficier de leur utilisation. Il s'agit de déplacer l'accent de la notion de propriété vers celle de « conservation » en prenant compte les responsabilités de toutes les parties prenantes, avec le partage des bienfaits comme élément essentiel. La « conservation » désigne ici la responsabilité de la sécurité et du bien-être d'une personne ou d'une chose. Cette notion implique des valeurs éthiques, telles que le soin, la curatelle (éthique médicale), la protection et la confiance, jusqu'à la tutelle ou la conservation en toute sécurité.

74. Dans ce contexte, les mégadonnées peuvent être considérées comme un bien commun de l'humanité. Les progrès scientifiques et technologiques et les nouvelles perspectives pourraient contribuer à résorber – et non à creuser – les inégalités qui empêchent de nombreuses personnes de jouir du meilleur état de santé susceptible d'être atteint, sur le plan national et international. Une telle approche est conforme aux paragraphes (f) et (g) de l'article 2 de la Déclaration universelle sur la bioéthique et les droits de l'Homme qui prévoient : « de promouvoir un accès équitable aux progrès de la médecine, des sciences et des technologies, ainsi que la plus large circulation possible et un partage rapide des connaissances concernant ces progrès et le partage des bienfaits qui en découlent, en accordant une attention particulière aux besoins des pays en développement » et « de sauvegarder et défendre les intérêts des générations présentes et futures » (UNESCO, 2005).

75. Le défi à l'avenir sera de créer la meilleure infrastructure de données afin qu'elles soient disponibles, accessibles et utilisables par tous dans le monde, et de développer de nouveaux modèles destinés à obtenir des profits économiques à travers des services ou à des dons paralléles ou complémentaires. Il faut renforcer la solidarité entre les citoyens, mais aussi chez les entreprises et les acteurs privés, afin qu'ils partagent ou cèdent leurs données et leurs résultats pour le bien commun. Les projets de « données ouvertes » et de « science ouverte » menés par plusieurs États, organisations non gouvernementales et sociétés privées reflètent déjà cet avenir proche, en ce sens qu'ils imaginent « une infrastructure de données optimale et accessible par tous dans le monde, un lieu majeur d'expérimentation, de découverte, et de création de modes de vie nouveaux et améliorés » (Nielsen, 2014).

76. Les concepts de responsabilité et de bien commun réaffirment le plaidoyer du CIB dans son Rapport sur le principe du partage des bienfaits : « [e]n acceptant l'idée que les droits de l'Homme sont universels, nous reconnaissons que ces progrès ne peuvent pas être un privilège. Le progrès ne doit pas servir à creuser les inégalités existantes entre les peuples et les pays. Dans le même temps, nous reconnaissons que c'est la solidarité à travers la participation et non la bienfaisance qui représente le lien de partage que nous devons encourager. Cela constitue la seule façon de concilier développement et respect pour tous » (UNESCO, 2015). Le rapport recommande également le renforcement des capacités, l'éducation scientifique, analyse l'impact de la « mobilité des cerveaux », l'accès libre aux données sur la santé, ainsi que l'autonomisation et la participation à la production des connaissances.

77. Plusieurs programmes ont été mis en place afin de renforcer les capacités des chercheurs et des instituts de recherche à travers le monde, notamment dans les pays en développement. Concernant les biobanques et la recherche génomique en Afrique, par exemple, l'initiative Hérédité Humaine et la Santé en Afrique (H3Africa) vise à renforcer l'expertise en génomique et sur les biobanquessur le continent, afin de lutter contre les problèmes de santé liés aux maladies transmissibles et non transmissibles (Consortium H3Africa, 2014). Cette initiative vise à donner aux scientifiques africains les moyens de contribuer efficacement aux projets scientifiques d'avant-garde et de devenir les chefs de file de la génomique, de la bio-informatique et de la science des données. Elle a pour finalité principale d'améliorer la santé de la communauté africaine et mondiale.

78. L'élaboration d'un cadre éthique régissant le partage des bienfaits découlant de l'utilisation des mégadonnées soulève la question de son application dans différents environnements. Cela dépendra en grande partie des circonstances de l'utilisation des données (recherche, soins de santé ou mode de vie), de la nature des bienfaits attendus et du type d'individus ou de groupes ayant un intérêt légitime à les utiliser. La mise en place d'un modèle de gouvernance à plusieurs niveaux peut couvrir tous les aspects de cette diversité ainsi que de la mise en balance des bénéfices et des risques de cadres spécifiques pour le partage des bienfaits (voir chapitre V). Ce modèle pourrait, par exemple, permettre de dégager des gains financiers considérables au bénéfice du groupe ayant fourni de nombreuses données afin de parvenir à une vision d'ensemble et à l'élaboration de nouveaux produits.

IV.4. Justice

IV.4.1. Fracture numérique

79. Les mégadonnées requièrent des outils et des fournisseurs d'accès et de gestion. La fracture numérique (également appelée « fossé numérique ») constitue l'un des obstacles majeurs à la démocratisation de l'information et de la communication, et donc au développement. Les technologies numériques contribuent amplement au développement et à la lutte contre la pauvreté, à tel point qu'elles figuraient dans le huitième objectif du Millénaire pour le développement (OMD) des Nations Unies relatif au renforcement du partenariat mondial pour le développement. Le fossé est désormais en train de se réduire. La cible 8.F visait à mettre les avantages de la technologie – notamment des TIC – à disposition de tous. Les OMD ont effectivement permis d'améliorer le niveau d'information des populations, notamment dans les zones les plus pauvres et les plus isolées. Dans le secteur de la santé, cette stratégie a contribué à renforcer la promotion de la santé et la prévention des maladies. Elle a également permis d'améliorer sensiblement l'accès aux prestations de soins, notamment via la télémédecine. Cette évolution favorise la sensibilisation et l'information des populations, sur lesquelles repose toute action de santé publique. Les bons résultats de la téléphonie mobile ont favorisé la mise en place de programmes de renforcement des connaissances et des compétences du grand public et des acteurs engagés dans la lutte contre les maladies non transmissibles. Citons, par exemple, le programme *Be Healthy Be Mobile*, lancé dans plusieurs pays, notamment au Costa Rica, en Égypte, en Inde, au Sénégal et en Zambie.

80. Le taux de couverture d'Internet a augmenté, passant d'un peu plus de 6 % de la population mondiale en 2000 à 48 % en 2017, et 53,6 % des ménages (Union internationale des télécommunications [UIT], 2017). 3,6 milliards de personnes sont donc connectées au réseau mondial d'applications et de contenus. Cependant, le débit Internet limité et les infrastructures nationales peu développées de nombreux pays à faible revenu limitent l'offre de services Internet à grande vitesse à un tarif raisonnable. Ces obstacles ont un impact concret sur les services et les applications accessibles aux internautes. C'est pourquoi les pays en développement et les pays les moins avancés rencontrent des difficultés à intégrer la gestion des mégadonnées dans leurs offres. En outre, le coût moyen des services reste souvent relativement élevé dans les pays les plus pauvres, où l'entretien et la mise à jour des outils (téléphones portables, etc.) sont parfois difficiles.

81. Bien que l'accès aux TIC se soit beaucoup amélioré, des écarts très importants persistent et tendent à se creuser entre et dans les pays. Le taux d'accès à Internet des ménages varie nettement en fonction de la situation économique du pays : en 2017, le taux de couverture est de 84,2 % en Europe, contre 18 % en Afrique (UIT, 2017). Seuls 41,3 % (soit moins de la moitié) de la population des pays en développement utilisent Internet, contre 81 % dans les pays développés (UIT, 2017). Pour cette raison, et bien que l'isolement et l'accessibilité des structures et des professionnels de santé soient considérés comme des enjeux prioritaires dans la plupart des pays en développement, la mise en œuvre de technologies innovantes et efficaces (téléexpertise, télédiagnostic ou téléconsultation, par exemple) est encore insuffisante en raison du manque de ressources.

82. Le niveau de compétence en matière de TIC, la culture numérique et l'offre de contenu local pertinent varient aussi très fortement d'un pays à l'autre. Même s'ils peuvent accéder aux contenus innovants grâce aux TIC, les pays en développement ne disposent pas des infrastructures et des ressources humaines nécessaires à leur adaptation et leur évaluation. Cette situation soulève des problèmes éthiques, entre autres le fait que le transfert massif des données ne soit assujetti à aucun cadre explicite (risque de « piratage des données ») ou aucune politique de gouvernance adaptée (Wyber *et al.*, 2015). De fait, d'énormes quantités de données sont transférées depuis les pays en développement, lesquels disposent de ressources humaines et techniques limitées, et sont traitées sans aucune garantie de protection de leur contenu.

IV.4.2. Non-discrimination

83. Dans de nombreux pays, l'accès aux soins repose non pas sur un modèle public, mais sur des modèles privés gérés par des assureurs privés, avec des degrés différents de participation, de contrôle et de suivi de la part des autorités publiques. Par conséquent, les personnes se voient parfois empêchées ou refusées l'obtention une couverture maladie en raison de la divulgation de données médicales les concernant. Si les compagnies d'assurance prennent connaissance en détail des risques encourus par un individu, on peut alors très difficilement parler d'un modèle d'assurance traditionnellement basé sur l'équilibre des risques collectifs, mais plutôt un modèle basé sur sur le profil détaillé des risques individuels.

84. Avec l'utilisation des TIC et des approches associées aux mégadonnées, de nouveaux modèles d'assurance réposant sur le comportement individuel font leur apparition dans différents domaines, y compris dans celui de l'assurance santé. Les personnes qui acceptent de communiquer régulièrement leurs données (par exemple sur leurs activités sportives, leurs habitudes alimentaires, etc.) par le biais de la géolocalisation, des objets connectés portables et des applications mobiles, se voient accorder des taux préférentiels ou d'autres avantages. Cette pratique risque de provoquer l'exclusion de trois catégories de personnes, qui ne pourront accéder aux avantages ou risquent, à long terme, d'être discriminées : (i) les personnes qui ne souhaitent pas communiquer leurs données personnelles à l'assureur, qu'elles soient en mesure ou non de répondre aux normes de comportement (par example, faire au moins 10 000 pas par jour) ; (ii) les personnes qui, indépendamment de leur souhait de communiquer ou non les données, ne peuvent répondre aux normes en raison d'un handicap, d'une maladie ou d'un grave événement, et qui ont précisément besoin de solidarité et d'un soutien social ; (iii) les personnes qui n'adhèrent pas à la notion de « santé » et de « vie saine », telle que définie par les compagnies d'assurance. L'autorité consistant à définir les comportements de santé à valoriser (faire au moins 10 000 pas par jour plutôt que de méditer tous les matins) ne devrait pas incomber aux compagnies d'assurance. Elle relève plutôt du domaine scientifique et social.

85. Il existe également un risque de discrimination résultant de possibles violations de l'anonymisation lors du traitement des mégadonnées entraîne également des risques de discrimination. L'agrégation des données ouvre la possibilité de la réidentification des personnes grâce au croisement des informations (origine ethnique, emplacement géographique, âge, dossiers médicaux, données génétiques) et d'autres métadonnées (Choudhury *et al.*, 2014).

86. Par ailleurs, il existe désormais des algorithmes puissants, capables d'établir le profil d'une personne même en l'absence de données personnelles la concernant, afin de regrouper les sujets selon des critères géographiques, socio-économiques, ethniques ou autres. L'anonymisation des données personnelles perd alors de son utilité si les résultats exposent les groupes auxquels ces personnes appartiennent à un risque de discrimination et de stigmatisation. Les membres d'une communauté n'ayant pas donné leur consentement ou n'ayant pas fourni leurs données, mais qui correspondent au profil d'un groupe défini, sont également exposés à ces risques.

87. En outre, la perte de liberté peut également être la conséquence d'une pression subtile exercée sur l'individu pour l'amener à modifier son comportement. Or, les prévisions se basent sur la fréquence du comportement. Par conséquent, les minorités (c'est-à-dire les personnes adoptant des comportements plus marginaux) risquent de devenir la cible de stigmatisation. Un autre risque est que les individus et certains groupes soient habilement contraints d'adopter les « comportements fréquents » pour ne pas être exclus.

88. Les approches en matière de mégadonnées soulèvent d'autres risques de stigmatisation et de désavantages structurels, évidents ou subtils, comme l'accès à la recherche et au progrès de ceux possédant des compétences et des moyens limités. Les algorithmes peuvent contenir des préjugés systématiques, pouvant même favoriser le racisme. Par conséquent, il est nécessaire de cartographier scrupuleusement les risques de

discrimination liés aux mégadonnées, en fonction du domaine et de la nature de la discrimination, et de prendre des mesures adaptées pour lutter contre la stigmatisation et la discrimination, au titre de l'article 11 de la Déclaration universelle sur la bioéthique et les droits de l'Homme.

IV.5. Durabilité énergétique et environnementale

89. Les mégadonnées relatives à la santé représentent également un enjeu écologique, au regard de leur coût énergétique et des avantages liés à une meilleure utilisation des ressources naturelles. L'accent est généralement mis sur les avantages potentiels offerts par les mégadonnées, notamment en ce qui concerne l'économie d'énergie et la lutte contre l'effet de serre (Carbon War Room, n.d.). Cependant, les technologies de l'information sont très énergivores et émettent des gaz à effet de serre tout au long de leur cycle de vie (Centre national de la recherche scientifique [CNRS], n.d.).

90. Les infrastructures assurant le fonctionnement des systèmes informatiques distribués et des solutions à distance sont très gourmandes en énergie et ont une empreinte carbone élevée. Elles consomment 10 % de l'énergie mondiale. La part de cette consommation liée à la santé est inconnue bien qu'elle soit probablement considérable. 38 % de cette consommation sont attribués aux terminaux, 14 % à la transmission et 48 % aux centres de données (Cappy, 2017). Il convient de noter que 80 % de la consommation énergétique des objets connectés (14 milliards aujourd'hui, 125 milliards en 2025) ne serait pas consacrée à leur utilisation, mais au maintien de la connectivité du réseau. Selon l'Agence internationale de l'énergie (AIE), la consommation des objets connectés dans le monde s'élevait à 616 térawatts-heures en 2013 (AIE, 2014), l'équivalent de la consommation annuelle de la Suède (10 millions d'habitants). Les centres de données hébergent des milliers de serveurs fonctionnant en continu. D'énormes quantités d'énergie sont nécessaires au fonctionnement, mais également au refroidissement des serveurs. Selon les estimations, les centres de données américains ont consommé 91 milliards de kilowatts-heures en 2013, une quantité qui serait suffisante pour approvisionner en électricité tous les ménages de New York pendant deux ans. À ce rythme, ce chiffre devrait atteindre 140 milliards de kilowatts-heures à l'horizon 2020 (Conseil de défense des ressources naturelles [NRDC], 2015).

91. L'égalisation de tension, les recherches sur l'informatique quantique, l'architecture des machines pour combler le fossé entre la gestion et le stockage des données, la modification de la tension des microprocesseurs ainsi que la bio-inspiration, qui cherche à améliorer le rapport coût-efficacité en s'inspirant de systèmes biologiques tels que le cerveau humain, peuvent constituer autant de sources d'amélioration.

92. La pollution due aux déchets d'équipements électriques et électroniques (DEEE) soulève également des inquiétudes sanitaires. On estime à 50 millions de tonnes le volume de DEEE produit chaque année dans le monde. Selon l'initiative Solving the E-waste Problem initiative (http://www.step-initiative.org/) à laquelle participent les Nations Unies, des groupes citoyens et des industriels, le volume total annuel de DEEE aura augmenté d'un tiers en 2017, pour atteindre 65,4 millions de tonnes.

93. L'impact écologique de la prospection et de l'exploitation des composants essentiels en vue de produire les 67 millions de tonnes de nouveaux équipements électriques et électroniques introduits sur le marché chaque année est également source d'inquiétude. Les « terres rares » désignent 17 éléments chimiques aux propriétés exceptionnelles : on leur doit la brillance des écrans d'ordinateur, les écrans tactiles des téléphones portables et la production d'électricité par les éoliennes. Malheureusement, l'extraction et le traitement des terres rares sont polluants, génèrent des déchets radioactifs et abîment le paysage. Ces problèmes ont déjà touché l'Indonésie et l'Australie.

IV.6. Recherche

94. Les mégadonnées pouvant constituer de puissants générateurs d'hypothèses, notamment dans le cadre des essais cliniques, il est fondamental que les recherches respectent les normes d'éthique, de protection des données et d'excellence les plus élevées. Les biobanques sont au cœur de la recherche biomédicale et constitue une source essentielle de mégadonnées au service de la recherche. Des guides de bonnes pratiques relatives à l'exploitation des mégadonnées aux fins de recherche académique impliquant la collecte d'échantillons et de données et leur stockage dans des biobanques ont déjà été publiées. Ils font l'objet de discussions régulières, publiées sous forme de recommandations émises par des organisations internationales, telles que l'Infrastructure européenne de recherche consacrée aux biobanques et aux ressources biomoléculaires en consortium (ERIC-BBMRI) (http://bbmri-eric.eu/) et l'OCDE. Parmi les améliorations récentes, citons : (i) la création de comités de représentants de patients, chargés d'examiner la procédure de gouvernance de la biobanque, notamment l'utilisation de la valeur commerciale éventuelle des données ; (ii) la mise en place d'une procédure de suivi, grâce à laquelle les patients sont tenus informés de la nature et des implications à long terme des travaux de recherche réalisés avec leurs données, et peuvent effectivement retirer leur consentement le cas échéant.

95. Le concept de « facteur d'impact associé aux bioressources » (Bioresource Research Impact Factor, BRIF) a été mis en place en vue de confirmer l'utilisation de bioressources de qualité (échantillons et données associées). L'initiative BRIF vise à faciliter le suivi de l'utilisation des données et des bases de données relatives aux échantillons biologiques. Les recommendations Citation of BioResources in journal Articles (CoBRA) ont été élaborées dans ce contexte : elles visent à encadrer et à normaliser la citation des bioressources dans la littérature académique. Elles peuvent également constituer un exemple d'approches des mégadonnées.

96. Assimilée à une capacité de « contrôle », la propriété des données implique le droit des personnes concernées à prévenir la manipulation des données, quelle qu'elle soit, notamment la pression sociale exercée sur les personnes pour les contraindre à approuver des utilisations inacceptables de leurs données (voir chapitre IV.3). Dans le cadre des biobanques et des bases de données, le contrôle permet, par exemple, de vérifier le caractère acceptable ou non de l'utilisation des données de recherche à des fins commerciales, par l'accès des entreprises privées et de tiers aux échantillons et aux données des biobanques. Inversement, la propriété des données peut être un obstacle à la recherche, par exemple en interdisant certaines formes d'analyses des données ou de méta-analyse. La législation nationale peut également avoir un rôle restrictif, notamment en interdisant le transfert de données.

97. Les efforts vers l'ouverture des données sont contradictoires à la protection des données médicalement sensibles. Dans ce contexte il faut également souligner que certaines revues scientifiques souhaitent recevoir et conserver l'intégralité des données utilisées pour l'obtention des résultats publiés par la revue, afin de permettre à d'autres chercheurs de reproduire les résultats ou de les utiliser dans le cadre de méta-analyses. Ce type de demande pose néanmoins problème : les éditeurs ou les autres propriétaires de ces types de dépôts peuvent choisir d'appliquer des droits ou des tarifs prohibitifs sur l'accès aux données conduisant à interdire ou décourager leur exploitation. Des projets de loi sont en cours de négociation dans plusieurs pays, en vue de permettre un accès libre aux données pour la recherche.

98. L'éducation des citoyens est un élément clé pour tirer le meilleur des mégadonnées recueillies à partir d'informations personnelles. Premièrement, pour que l'exercice du droit d'accès prenne tout son sens, les sujets consentant à ce que leurs données personnelles soient utilisées à des fins de recherche doivent être réellement en mesure de faire valoir ce droit moyennant des efforts raisonnables. Deuxièmement, les mégadonnées exigent des

connaissances scientifiques pointues qui ne s'acquièrent que par l'éducation, afin d'éviter tout malentendu (par exemple concernant l'interprétation des résultats d'une analyse).

99. Il existe un risque de confiance excessive dans le pouvoir des métadonnées, risque d'autant plus important qu'on assiste depuis peu à l'émergence d'une relation directe entre les gestionnaires des bases de données et les patients/citoyens, hors de toute intervention médicale. Si cette pratique est absente du champ académique, elle se développe rapidement dans la recherche privée menée par des entreprises commerciales. Les interventions et les interprétations médicales sont indispensables dans la mesure où les prédictions fondées sur les analyses de mégadonnées ne considèrent pas tout ce qui devrait être traité. De fait, l'interprétation de la signification des résultats obtenus grâce aux mégadonnées pour une personne donnée restent l'un des objectifs fondamentaux de la relation entre le médecin et son patient.

100. L'analyse des mégadonnées peut produire des résultats potentiellement utiles pour la santé du patient, qui sont parfois appelés découvertes fortuites ou non sollicitées. Ces questions ayant déjà été traitées dans le Rapport du CIB sur le principe de non-discrimination et de non-stigmatisation (UNESCO, 2014), il n'est pas nécessaire de les étudier à nouveau.

101. En matière de recherche en santé publique, les mégadonnées permettront de mettre en place des politiques publiques visant à promouvoir la santé et prévenir les maladies au niveau collectif. Des garanties suffisantes doivent être mises en place pour protéger le droit des individus à la vie privée et doivent respecter les principes de bonne gouvernance concernant l'utilisation des données. Le coût d'acquisition, de maintenance et d'utilisation des mégadonnées aux fins de politiques de santé publique est un autre écueil majeur, notamment dans les pays en développement aux ressources limitées.

102. La recherche médicale se sert désormais de dispositifs personnels connectés à Internet (smartphones) à des fins de suivi pour collecter des données de santé (santé mobile). Si cette pratique peut constituer une source utile de données de vie réelle, elle pose toutefois un problème d'ordre éthique : le risque d'exploitation inappropriée des données ou de violation du droit à l'autonomie, les téléphones portables pouvant accumuler une mine d'informations personnelles de toute sorte sur l'utilisateur, avec peu de garanties pour protéger l'autonomie et la vie privée. L'utilisation de ces appareils électroniques pour mener des recherches et des enquêtes relatives à la santé peut néanmoins s'avérer efficace et performante tant que des garanties suffisantes sont appliquées pour protéger l'autonomie et la vie privée des personnes.

V. GOUVERNANCE

103. Les systèmes de gouvernance s'appliquant aux mégadonnées doivent protéger les droits fondamentaux des personnes dont elles proviennent, notamment leur liberté à prendre des décisions, et doivent viser à maintenir la confiance du public. Les principes directeurs de la gouvernance doivent par conséquent inclure le respect de l'autonomie et le droit à l'information, le respect de la volonté, le respect de la vie privée, l'égalité et la licéité. La gouvernance des données doit garantir que la participation et l'engagement citoyen et le partage des données ne feront pas l'objet d'exploitation, de manipulation et de contrôle indus. Les recommandations du CIB sont fondées sur ces principes.

104. Par ailleurs, les politiques de santé publique doivent trouver le juste équilibre entre les intérêts et les droits individuels et ce que l'on appelle « bien public ». S'agissant des mégadonnées, la plupart des acteurs recueillant et utilisant les données n'ont pas été investis, par les personnes dont les renseignements sont intégrés (volontairement ou involontairement) aux bases de données, d'un mandat démocratique pour définir en quoi consiste réellement le « bien public ». Il en résulte des conflits d'ordre éthique que seule une structure de gouvernance appropriée et à même de garantir un « bien public » peut éviter.

105. La portée mondiale des mégadonnées et de la santé, l'immense diversité et la multiplication rapide des acteurs du secteur, ainsi que la rapidité du progrès technologique rendent difficile l'instauration d'une réglementation exhaustive et équilibrée. Toutefois, une gouvernance prudente s'impose – à des niveaux et selon des méthodes multiples – pour garantir un usage bénéfique, veiller à des comportements responsables et éviter les préjudices. Elle permettra d'orienter et d'encadrer les diverses parties prenantes et institutions, par le biais de mesures juridiques et non juridiques (règles, règlements, décrets, accords, codes de conduite autocontraignants, etc.).

106. À l'ère des mégadonnées, il est de plus en plus difficile d'imaginer que la protection des données puisse uniquement être régulée par l'adhésion au consentement ou à l'anonymisation, sans autre garantie (voir chapitre sur l'autonomie). Cela nous amène à la conclusion suivante : il est impératif de créer et de mettre en œuvre une structure de gouvernance exhaustive à plusieurs niveaux qui permette une utilisation responsable des données. Il sied également de noter que, comme il a déjà été indiqué au paragraphe 35, si les individus deviennent de plus en plus transparents en raison de l'accumulation des données personnelles, les systèmes, eux, se caractérisent par une opacité croissante. Les cadres de gouvernance doivent gagner en transparence afin de lutter contre cette tendance. Plusieurs modèles sont envisageables. Cependant, il doit s'agir impérativement d'une structure publique ou, au moins, d'un partenariat public-privé. La véritable participation des patients et du grand public à la mise en place et à l'application de la gouvernance est une condition préalable.

107. La transparence des algorithmes (qui sont pour le moment opaques) est un élément essentiel dans ce contexte. Les institutions et les entreprises doivent faire preuve de transparence à l'égard des algorithmes sur lesquels elles s'appuient. En ce qui concerne les décisions prises à l'aide d'algorithmes, il faut expliquer les procédures suivies par l'algorithme et les éléments ayant conduit aux décisions qui ont été prises. Certains prônent également la publication du code source des algorithmes. Cependant, les droits de propriété intellectuelle et les aspects technologiques, par exemple ceux liés aux algorithmes d'apprentissage automatique, doivent être pris en compte au moment d'élaborer des systèmes appropriés de transparence et de contrôle.

108. Le droit fondamental à la protection des données offre un socle théorique et juridique qui garantit l'acceptabilité de l'utilisation des données sur le plan moral et juridique, et qui met en place un cadre réglementaire complexe de gouvernance de l'information. La licéité, un principe clé en matière de protection des données, exige que tout traitement des données personnelles soit juridiquement recevable. Il s'appuie sur le système général d'équilibre des pouvoirs, lequel réglemente les activités de traitement des données personnelles. Il vise à compléter les droits individuels, garantis par le droit fondamental au respect de la vie privée, en attribuant des responsabilités et des obligations concrètes aux utilisateurs de données. Le principe de licéité a un statut juridique différent dans les différents pays.

109. Ce cadre de gouvernance doit prévoir les dispositions réglementaires et des normes éthiques pour toutes les étapes de la boucle cybernétique, y compris la collecte, l'accès, la publication, le recoupement, l'analyse et la réutilisation des données, etc. Dans le contexte des considérations éthiques et juridiques, les éléments suivants sont perçus comme essentiels pour un tel cadre.

a. Formulation claire de la finalité de la base de données.
b. Procédures de recherche du consentement (global), de reprise de contact (y compris le retour des résultats) et de nouvelle recherche du consentement.
c. Procédure de non-consentement, en cas d'opposition.
d. Dispositions visant à garantir le respect du droit d'accès aux données, de rectification et d'effacement.
e. Modalités de retrait, en précisant le degré de faisabilité technique de l'opération.

f. Dispositions relatives à la protection de la vie privée, incluant au minimum une délimitation de ladite protection.

g. Politiques applicables après le décès du participant.

h. Dispositions relatives à la propriété des données et des produits associés.

i. Dispositions relatives à la collecte, au stockage et à la durée de stockage des données, notamment le contrôle qualité et les garanties de protection de la vie privée et de la confidentialité.

j. Dispositions relatives à l'accès aux données, notamment le partage des données, et aux conditions d'accès.

k. Rôle des comités d'éthique de la recherche (CER) et des comités d'accès aux données (CAD) dans les prises de décisions relatives au partage de données.

l. Dispositions relatives à la gestion des données en cas de transfert de propriété ou de clôture de la base de données.

m. Transparence des algorithmes utilisés dans la reconnaissance des séries ; dispositions relatives à la vérification du profilage des individus et des groupes conformément aux considérations éthiques.

n. Publicité des intérêts commerciaux et collaboration avec les acteurs commerciaux.

o. Dispositions permettant aux participants de se tenir informés de l'utilisation en cours et ultérieure de leurs données, y compris aux fins de recherche.

p. Politique claire relative à la divulgation des résultats de recherche individuels et groupés aux participants.

q. Dispositions relatives à l'implication des participants dans la conception des procédures de gouvernance, notamment en ce qui concerne le contrôle éthique et la communication avec les fournisseurs de données.

r. Dispositions relatives au partage des bienfaits.

s. Dispositions relatives aux populations autochtones/locales et aux minorités traditionnelles.

t. Les enfants et les adolescents qui atteignent l'âge de la maturité pendant le projet de recherche devraient se voir offrir l'opportunité de donner un consentement informé pour la continuation du stockage et de l'utilisation de leurs données, et devraient également être capables de retirer leur consentement pour de futures recherches.

110. Les éléments décrits ci-dessous pourront jeter les bases de futurs traités internationaux et d'accords autocontraignants entre les fournisseurs, voire déboucher sur la création d'un organisme international de vigilance. Des entités déjà existantes comme les comités d'éthique de la recherche (CER), les comités d'accès aux données (CAD) et les organismes de protection des données peuvent jouer un rôle important dans la mise en œuvre de ce cadre de gouvernance à plusieurs niveaux régissant les relations entre un grand nombre de parties prenantes.

111. Le CIB recommande aux États membres d'adopter un instrument juridique international sur la protection des données. Il est disposé, au besoin, à contribuer à l'élaboration d'un cadre de gouvernance adéquat en amont dudit traité. Chaque État pourra ensuite instaurer sa propre législation nationale, et mettre en place un organisme de supervision des systèmes de gouvernance. Ce dernier constituera également un point d'entrée clair aux fins de contrôle public.

VI. RECOMMANDATIONS

112. Afin que les mégadonnées contribuent positivement à la santé mondiale et que leurs avantages soient optimisés dans les soins et de la recherche de santé sans qu'il y ait violation

des droits fondamentaux inscrits dans la Déclaration universelle des droits de l'Homme et dans la Déclaration universelle sur la bioéthique et les droits de l'Homme, le CIB formule les recommandations suivantes.

113. Compte tenu de la complexité, de la portée mondiale et de la grande diversité des parties prenantes à l'utilisation des mégadonnées liées à la santé, une coopération internationale ainsi qu'une approche de gouvernance à plusieurs niveaux sont fondamentales si l'on souhaite parvenir à un équilibre entre confiance et contrôle au bénéfice de tous (pour de plus amples informations, voir chapitre V).

114. Le CIB considère quatre domaines essentiels dans lesquels des efforts doivent être déployés afin de garantir la protection des droits des individus et de favoriser l'intérêt général, reconnaissant le fait que les individus perdent inévitablement le contrôle sur l'utilisation de leurs données avec l'arrivée des mégadonnées : la gouvernance, l'éducation, le renforcement des capacités et le partage des bienfaits.

115. Dans le présent chapitre, le CIB présente des exemples de mesures importantes. Celles-ci constituent une étape du débat international en cours et concernent différentes parties prenantes. Leur réussite finale dépend de la coopération et la participation extensives de toutes les parties prenantes, y compris les patients, les participants aux recherches, les utilisateurs et les citoyens en général.

116. Les organisations internationales sont appelées à concevoir et à appuyer un cadre international régissant l'utilisation des mégadonnées dans les domaines liés à la santé, notamment les soins de santé et la recherche médicale. Le CIB recommande notamment :

a. aux Nations Unies d'élaborer et d'adopter un instrument juridique international sur la protection des données dans le domaine des soins de santé et de la recherche en santé ;

b. à l'UNESCO d'élaborer une convention sur la protection de la vie privée, notamment un cadre régissant les nouvelles approches de propriété et de conservation des données personnelles qui concerne, entre autres, les données de santé. Celle-ci devrait également aborder le traitement des données personnelles et la présence numérique d'une personne après sa mort physique. Cette convention peut s'appuyer sur le projet de résolution du Conseil des droits de l'Homme relatif au droit à la vie privée à l'ère du numérique (A/HRC/34/L.7/Rev.1) ;

c. à l'OMS d'encourager l'établissement d'un accord avec les fournisseurs d'applications garantissant l'autonomie de la personne et la transparence des applications liées à la santé ainsi que le caractère approprié des informations utilisées ;

d. la mise en place d'un système mondial de vigilance sur l'utilisation que font les applications liées à la santé des mégadonnées ;

e. la mise en place d'infrastructures de données publiques ; une mesure nécessaire pour que les accords internationaux entendent les mégadonnées comme un bien commun de l'humanité et facilitent, dans la mesure du possible, leur accès libre et leur utilisation dans l'intérêt du bien commun ;

f. à l'OCDE d'élaborer un cadre régissant le partage des bienfaits tirés des applications utilisant les mégadonnées. Cela devrait également contribuer à l'élimination de la fracture numérique ;

g. aux organismes internationaux ainsi qu'aux organismes régionaux et nationaux qui établissent les normes techniques applicables aux appareils et applications dans le contexte des mégadonnées de définir ces normes conformément aux principes éthiques de respect de l'autonomie, de la vie privée et de la justice, comme expliqué dans le présent rapport, ainsi que du besoin de transparence ;

h. Il est fait appel à l'Agence internationale de l'énergie (AIE) pour unir les efforts en faveur d'un usage durable et responsable de l'énergie dans la gestion des mégadonnées. Elle pourrait mettre en place des programmes pour développer des politiques d'efficacité énergétique incluant un dialogue avec des pays non-membres ;

i. Les agences de protection de l'environnement telles que le Programme des Nations Unies pour l'Environnement ainsi que l'OMS sont appelées à mettre en place un plan d'action coordonné pour sauver les ressources rares. En outre, elles doivent mettre en œuvre un programme pour éviter les E-déchets qui impactent la santé des personnes particulièrement dans les pays en voie de développement.

117. Le CIB appelle les pouvoirs publics à élaborer et mettre en œuvre un plan d'action (prévoyant législation et politiques) englobant, entre autres, les aspects suivants :

a. la mise en œuvre harmonisée à l'échelle internationale de principes de protection des données mondialement reconnus ;

b. les gouvernements nationaux – dans la mesure où cela n'a pas été déjà fait – sont appelés à établir une Agence de contrôles des données efficace. Toutes les Agences de contrôle des données doivent travailler ensemble avec le système mondial de vigilance sur l'utilisation que font les applications liées à la santé des mégadonnées susmentionné (paragraphe 116[d]). Ce système coordonné pourrait servir de point de départ pour l'instrument juridique international sur la protection des données dans le domaine des soins de santé et de la recherche en santé ;

c. le renforcement des capacités associées à l'utilisation des mégadonnées dans le domaine de la santé et de la recherche médicale (y compris la mise en place d'une infrastructure de données efficace) ;

d. la promotion de systèmes d'apprentissage croisé qui utilisent les données issues des soins de santé quotidiens pour développer les soins de santé de demain ;

e. la mise en place d'une coopération transfrontalière efficace concernant le traitement des données de santé à caractère personnel dans l'intérêt public en matière de santé ;

f. la promotion de l'éducation, à savoir l'acquisition de connaissances et de compétences en matière de mégadonnées et la sensibilisation aux conséquences éthiques significatives de leur utilisation. Une attention particulière doit notamment être accordée aux groupes vulnérables, tels que les mineurs et les personnes à capacité réduite ;

g. la mise en place de différents modèles de consentement adaptés au contexte des soins et de la recherche en santé, autorisant un consentement global et dynamique quand ils sont, réalisables et protégés par des garanties. Il en va de même pour le consentement électronique ;

h. la protection par défaut de la vie privée des individus partageant leurs données, et la conception d'appareils et d'équipements technologiques respectueux de la vie privée. Une attention particulière doit être portée à la protection de la vie privée des groupes, notamment en ce qui concerne les multiples possibilités de discrimination ;

i. la mise en place d'un CER ou d'une institution similaire afin de surveiller l'utilisation des mégadonnées dans la recherche commerciale ;

j. l'élaboration et l'application d'instruments tenant compte des spécificités culturelles et favorisant l'engagement véritable du public et des patients ;

k. les gouvernements doivent lancer des programmes coordonnés qui motivent les développeurs d'appareils à créer des protocoles de communication qui

permettent des économies d’énergie. Une des priorités doit être de standardiser les procedures pour la collecte et la gestion des données.

118. Le CIB appelle les multiples institutions de santé et de recherche ainsi que les entreprises à élaborer des directives, des codes de conduite et des instruments autocontraignants adaptés au contexte et visant tout particulièrement à régir les applications utilisant les mégadonnées. Des politiques éthiques et des codes de conduite ciblant les professionnels de la santé, les informaticiens, les chercheurs cliniciens, les scientifiques des données et les autres parties prenantes du milieu doivent également être élaborés. La plus haute priorité est d’encourager l’adoption de comportements éthiques, sans négliger les conséquences en cas de violation des principes éthiques.

BIBLIOGRAPHIE

Agence européenne des médicaments (EMA), 2016, *External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use*, Londres, EMA. Disponible à l'adresse : http://www.ema.europa.eu/docs/en_GB/document_library/Regulatory_and_procedural_guideline/2016/03/WC500202621.pdf.

Agence internationale de l'énergie (AIE), 2014, *More Data, Less Energy: Making Network Standby More Efficient in Billions of Connected Devices*, Paris, AIE. Disponible à l'adresse : https://www.iea.org/publications/freepublications/publication/MoreData_LessEnergy.pdf.

Andanda, P., Wathuta, J., Leisinger, K. et Schroeder, D., 2016, *National and International Compliance Tools*, *a report for the TRUST Project*. Disponible à l'adresse : http://trust-project.eu/wp-content/uploads/2017/02/TRUST-664771-National-and-International-Compliance-Tools-Final.pdf.

Association médicale mondiale (AMM), 2013, *Déclaration d'Helsinki de l'AMM — Principes éthiques applicables à la recherche médicale impliquant des êtres humains* (en ligne). Disponible à l'adresse : https://www.wma.net/fr/policies-post/declaration-dhelsinki-de-lamm-principes-ethiques-applicables-a-la-recherche-medicale-impliquant-des-etres-humains/.

AMM, 2016, *Déclaration de l'AMM sur les considérations éthiques concernant les bases de données de santé et les biobanques* (online). Disponible à l'adresse : https://www.wma.net/fr/policies-post/declaration-de-lamm-sur-les-considerations-ethiques-concernant-les-bases-de-donnees-de-sante-et-les-biobanques/.

Bowker, G. C., 2014, « Big data, big questions the theory/data thing », *International Journal of Communication*, Los Angeles, USC Annenberg Press, Vol. 8, p. 1795-1799.

Cappy, A., 2017, « Impact énergétique des Big Data », in Bouzeghoub, M. et Mosseri, R. (dir.), *Les Big Data à découvert*, Paris, CNRS.

Carbon War Room., n.d., *Carbon War Room* (en ligne). Disponible à l'adresse : http://carbonwarroom.com/.

Centre national de la recherche scientifique, n.d., *EcoInfo* (en ligne), Paris, CNRS. Disponible à l'adresse : http://ecoinfo.cnrs.fr/.

Choudhury, S., Fishman, J. R., McGowan, M. L. et Juengst, E. T., 2014, « Big data, open science and the brain: Lessons learned from genomics », *Frontiers in Human Neuroscience*, 8, p. 239, DOI : 10.3389/fnhum.2014.00239.

Cohen, J. E., 2013, « What privacy is for », *Harvard Law Review*, Cambridge, Harvard Law Review, vol. 126, n° 7, p. 1904-1933.

Coles, D., Wathuta, J. et Andanda, P., 2016, « ICT and Mobile Data for Health Research », in Schroeder, D., Cook Lucas, J., Fenet S. et Hirsch, F. (dir.),*"Ethics Dumping"- Paradigmatic Case Studies*, *a report for TRUST*. Disponible à l'adresse : http://trust-project.eu/wp-content/uploads/2016/03/TRUST-664771-Paradigmatic-Case-Studies-WP1-Final.pdf.

Comitato Nazionale per la Bioetica (CNB), 2016, *Information and Communication Technologies and Big Data: Bioethical Issues,* Rome, CNB. Disponible à l'adresse : http://bioetica.governo.it/media/172149/p124_2016_information-techonolgies-and-big-data_en.pdf.

Commission européenne (CE), 2012, *Opinion No. 26: Ethics of Information and Communication Technologies*, Groupe européen d'éthique des sciences et des nouvelles technologies (EGE), Luxembourg, Office des publications de l'Union européenne. Disponible à l'adresse : http://bookshop.europa.eu/fr/ethics-of-information-and-communication-technologies-pbNJAJ12026/.

CE, 2015, Opinion No. 29 : The ethical implications of new health technologies and citizen participation, Groupe européen d'éthique des sciences et des nouvelles technologies (EGE), Luxembourg, Office des publications de l'Union Européenne. Disponible à l'adresse : https://publications.europa.eu/en/publication-detail/-/publication/e86c21fa-ef2f-11e5-8529-01aa75ed71a1/language-en/format-PDF/source-39541144.

Conférence des Nations Unies sur le commerce et le développement (CNUCED), 2016, *Data protection regulations and international data flows: Implications for trade and development*, Genève, CNUCED. Disponible à l'adresse : http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

Conseil de l'Europe, 1950, *Convention de sauvegarde des droits de l'Homme et des libertés fondamentales* (Convention européenne des droits de l'Homme), Strasbourg, Conseil de l'Europe. Disponible à l'adresse : http://www.echr.coe.int/pages/home.aspx?p=basictexts&c=fre.

Conseil de l'Europe, 1981, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, Conseil de l'Europe. Disponible à l'adresse : http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108.

Conseil de l'Europe, 2001, *Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données*, Strasbourg, Conseil de l'Europe. Disponible à l'adresse : http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/181.

Conseil de Nuffield sur la bioéthique, 2015, *The collection, linking and use of data in biomedical research and health care: ethical issues*, Londres, Nuffield Council on Bioethics. Disponible à l'adresse : http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf.

Consortium H3Africa, 2014, « Research capacity. Enabling the genomic revolution in Africa », *Science,* New York, American Association for the Advancement of Science (AAAS), vol. 344, n° 6190, p. 1346-1348.

Coopération économique des pays d'Asie-Pacifique, 2015, *Updates to the APEC Privacy Framework*, Singapour, secrérariat de l'APEC. Disponible à l'adresse : http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf.

Coordinated Research Infrastructures Building Enduring Life-science Services, n.d. Disponible à l'adresse : http://www.corbel-project.eu/home.html.

Cour de justice européenne (CJE), 2012, *Arrêt de la Cour (grande chambre) : Used Soft GmbH contre Oracle International Corp. (C-128/11), Luxembourg, CJE.* Disponible à l'adresse : http://curia.europa.eu/juris/document/document.jsf?docid=124564&doclang=FR.

États-Unis, 1996, *Health Insurance Portability and Accountability Act*. Washington D.C., Congrès des États-Unis. Disponible à l'adresse : https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

États-Unis, 2002, *HIPAA Privacy Rule*, Washington D.C., Département de la Santé et des Services sociaux des États-Unis. Disponible à l'adresse : https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es.

États-Unis, 2009, *The American Recovery and Reinvestment Act*. Washington D.C., Congrès des États-Unis. Disponible à l'adresse : https://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf.

États-Unis, 2014, *Big Data: Seizing Opportunities, Preserving Values*, Washington D.C., Bureau exécutif du président des États-Unis. Disponible à l'adresse : https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

États-Unis, n.d., *Privacy Shield Program Overview* (en ligne). Washington D.C., Département du Commerce des États-Unis. Disponible à l'adresse : https://www.privacyshield.gov/Program-Overview.

Hoeren, T., 2014, « Big Data and the Ownership in Data: Recent Developments in Europe », *European Intellectual Property Review*, Londres, Sweet & Maxwell, vol. 36, nº 12, p. 751-754.

Initiative en matière de médicaments innovants (IMI), 2014, *Code of Practice on Secondary Use of Medical Data in Scientific Research Projects*, projet final du 27 août 2014. Disponible à l'adresse : http://www.imi.europa.eu/sites/default/files/uploads/documents/CodeofPractice_SecondaryUseDRAFT.pdf.

Institute of Medicine, 2007, *The Learning Healthcare System: Workshop Summary*, Washington D.C., The National Academies Press.

Institute of Medicine, 2013, *Best care at lower cost: The path to continuously learning health care in America*, Washington D.C., The National Academies Press.

International Data Corporation (IDC), 2014, *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, Executive Summary: Data Growth, Business Opportunities, and the IT Imperatives* (en ligne). Disponible à l'adresse : https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.

Kaplan, W., Wirtz, V. J., Mantel-Teeuwisse, A., Stokl, P., Duthey, B. et Laing, R., 2013, *Priority Medicines for Europe and the World: 2013 Update*, Genève, OMS. Disponible à l'adresse : http://www.who.int/medicines/areas/priority_medicines/MasterDocJune28_FINAL_Web.pdf?ua=1.

Laurie, G., Ainsworth, J., Cunningham, J., Dobbs, C., Jones, K. H., Kalra, D., Lea, N. C. et Sethi, N., 2015, « On moving targets and magic bullets: Can the UK lead the way with responsible data linkage for health research? », *International Journal of Medical Informatics*, Amsterdam, Elsevier, vol. 84, nº 11, p. 933-940.

Lavenex, S. et Schimmelfennig, F., 2009, « EU rules beyond EU borders: theorizing external governance in European politics », *Journal of European Public Policy*, vol. 16, nº 6, p. 791-812.

Lea, N. C., 2015, *Design and Development of a Knowledge Modelling Approach to Govern the Use of Electronic Health Records for Research*, thèse de doctorat, University of London, Royaume-Uni.

Mertz M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C. and Woopen, C. 2016. *Digitale Selbstbestimmung*. Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health. DOI 10.8716/ceres/00001.

Mittelstadt, B. D. et Floridi L., 2016, « The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts », *Science and Engineering Ethics*, New York, Springer, vol. 22, p. 303-341.

Mostert, M., Bredenoord, A. L., Biesaart, M. C. I. H. et van Delden, J. J. M., 2015, « Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach », *European Journal of Human Genetics*, Londres, Nature Publishing Group, vol. 24, N° 7, pp. 956-960, DOI : 10.1038/ejhg.2015.239.

Nations Unies, 1948, *Déclaration universelle des droits de l'Homme*, New York, Nations Unies. Disponible à l'adresse : http://www.un.org/fr/universal-declaration-human-rights/index.html.

Nations Unies, 1990, *Principes directeurs pour la réglementation des fichiers personnels informatisés*, adoptés par la résolution 45/95 de l'Assemblée générale des Nations Unies le 14 décembre 1990, New York, Nations Unies. Disponible (en anglais) à l'adresse : http://www.refworld.org/pdfid/3ddcafaac.pdf.

Natural Resources Defense Council, 2015, *America's Data Centers Consuming and Wasting Growing Amounts of Energy* (en ligne), New York, NRDC. Disponible à l'adresse : https://www.nrdc.org/resources/americas-data-centers-consuming-and-wasting-growing-amounts-energy.

Nielsen, M., 2014, *Who Owns Big Data?* (en ligne), BBVA OpenMind. Disponible à l'adresse : https://www.bbvaopenmind.com/wp-content/uploads/2014/02/BBVA-OpenMind-Technology-Innovation-Internet-Bussines-Michael-Nielsen-Who-Owns-Big-Data.pdf.

OCDE, 2010, *Améliorer l'efficacité du secteur de la santé : Le rôle des technologies de l'information et des communications*, Paris, OCDE. Disponible à l'adresse : http://www.oecd-ilibrary.org/social-issues-migration-health/ameliorer-l-efficacite-du-secteur-de-la-sante_9789264084636-fr.

OCDE, 2013a, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Paris, OCDE. Disponible à l'adresse : http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm.

OCDE, 2013b, *Strengthening Health Information Infrastructure for Health Care Quality Governance : Good Practices, New Opportunities and Data Protection Challenge*s, Paris, OCDE. Disponible à l'adresse : http://www.oecd.org/publications/strengthening-health-information-infrastructure-for-health-care-quality-governance-9789264193505-en.htm.

OCDE, 2015, *Health Data Governance: Privacy, Monitoring and Research*, Paris, OCDE. Disponible à l'adresse : http://www.oecd.org/fr/publications/health-data-governance-9789264244566-en.htm.

OCDE, 2017, *OECD Recommendation on Health Data Governance*, Paris, OCDE. Disponible à l'adresse : http://www.oecd.org/els/health-systems/health-data-governance.htm.

OMS, 2011, « mHealth ou santé mobile : de nouveaux horizons pour la santé grâce aux technologies mobiles », Genève, OMS. Disponible (en anglais) à l'adresse : http://apps.who.int/iris/bitstream/10665/44607/1/9789241564250_eng.pdf.

OMS, n.d., *eHealth* (en ligne). Disponible à l'adresse : http://www.who.int/ehealth/en/.

Organisation mondiale du commerce, 1994, *Accord sur les Aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC)*, Genève, OMC. Disponible à l'adresse : https://www.wto.org/french/tratop_f/trips_f/intel2_f.htm.

Pharmaceutical Research and Manufacturers of America (PhRMA)/Fédération européenne des industries pharmaceutiques (EFPIA), 2013, *Principles for Responsible Clinical Trial Data Sharing* (en ligne). Disponible à l'adresse : http://transparency.efpia.eu/uploads/Modules/Documents/data-sharing-prin-final.pdf.

Rathenau Instituut, 2017, *Human rights in the robot age. Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality*, La Haye, Rathenau Instituut. Disponible à l'adresse : https://www.rathenau.nl/en/publication/human-rights-robot-age-challenges-arising-use-robotics-artificial-intelligence-and.

Science International, n.d., « Open Data in a Big Data World », Paris, Conseil international de la science (ICSU), Conseil international des sciences sociales (ISSC), World Academy of Sciences (TWAS), InterAcademy Partnership (IAP). Disponible à l'adresse : http://www.science-international.org/.

Sethi, N. et Laurie, G., 2013, « Delivering proportionate governance in the era of eHealth: making linkage and privacy work together », *Medical Law International*, Thousand Oaks, SAGE Publications, vol. 13, nº 2-3, p. 168–204.

Shilton, K., 2009, « Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection », *Communications of the ACM*, New York, ACM, vol. 52, nº 11, p. 48-53.

UNESCO, 2005, *Déclaration universelle sur la bioéthique et les droits de l'Homme*, Paris, UNESCO. Disponible à l'adresse : http://portal.unesco.org/fr/ev.php-URL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html.

UNESCO, 2014, *Rapport du CIB sur le principe de non-discrimination et de non-stigmatisation*, Paris, UNESCO. Disponible à l'adresse : http://unesdoc.unesco.org/images/0022/002211/221196f.pdf.

UNESCO, 2015, *Rapport du CIB sur le principe du partage des bienfaits,* Paris, UNESCO. Disponible à l'adresse : http://unesdoc.unesco.org/images/0023/002332/233230F.pdf.

Union africaine, 2014, *Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel*, Addis-Abeba, UA. Disponible à l'adresse : https://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Union européenne, 1995, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, Journal officiel de l'Union européenne (en ligne). Disponible à l'adresse : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A31995L0046.

Union européenne, 1996, *Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données*, Journal officiel de l'Union européenne (en ligne). Disponible à l'adresse : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31996L0009.

Union européenne, 2015, *Règlement général sur la protection des données* (texte de compromis à l'issue du trilogue) (en ligne). Disponible (en anglais) à l'adresse : http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.

Union européenne, 2016, *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, Journal officiel de l'Union européenne (en ligne). Disponible à l'adresse : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

Union internationale des télécommunications, 2015a, *ICT Facts and Figures 2015,* Genève, UIT. Disponible à l'adresse : http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

Union internationale des télécommunications, 2015b, *ITU's Annual Report 2015,* Genève, UIT. Disponible à l'adresse : http://www.itu.int/en/annual-report-2015/Pages/default.aspx.

Union internationale des télécommunications, 2016, *ICT Facts and Figures 2016,* Genève, UIT. Disponible à l'adresse : http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

Union internationale des télécommunications, 2016b, *ITU's Annual Report 2016*, Genève, UIT. Disponible à l'adresse : http://www.itu.int/en/annual-report-2016/Pages/default.aspx.

Union internationale des télécommunications, 2017, *ICT Facts and Figures 2017*, Genève, UIT. Disponible à l'adresse : http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf

Vayena, E. et Tasioulas, J., 2015, « "We the Scientists": a Human Right to Citizen Science? », *Philosophy & Technology*, New York, Springer, vol. 28, n° 3, p. 479–485.

Weiss, M. A. et Archick, K., 2016, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, Washington D.C., Service de recherche du Congrès des États-Unis. Disponible à l'adresse : https://fas.org/sgp/crs/misc/R44257.pdf.

Wyber R., Vaillancourt, S., Perry, W., Mannava, P., Folaranmi, T., Celi, L. A., 2015, « Big Data in global health: improving health in low- and middle-income countries? », *Bulletin de l'Organisation mondiale de la Santé*, Genève, OMS, vol. 93, p. 203-208, DOI : http://dx.doi.org/10.2471/BLT.14.139022.