En collaboration avec
université McGill

WORLD ECONOMIC FORUM

Façonner l'avenir de l'Internet des corps: Nouveaux défis technologiques

la gouvernance

BRIEFINGPAPER

JUILLET 2020

Couverture: Unsplash / Umberto

Contenu

3 Préface

4 Résumé

6 1 Première partie: l'Internet des corps est là

7 1.1 Gamme et catégories de technologies

8 1.2 Avantages sociaux basés sur les données

dix 1,3 Les risques liés à l'internet des corps

13 2 Deuxième partie: Gouvernance des données de l'internet des organismes

14 2,1 Paysage réglementaire des données aux États-Unis et dans l'UE

18 2.2 Nouveaux défis de gouvernance à l'ère du big data

21 2,3 Envisager les possibilités et les options

23 Contributeurs

25 Notes de fin

© 2020 Forum économique mondial. Tous les droits sont réservés. Aucune partie de cette publication ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit, y compris la photocopie et l'enregistrement, ou par tout système de stockage et de recherche d'informations.

Préface

Alors que les nouvelles technologies s'intègrent au corps humain, les opportunités - et les risques - abondent.

Xiao Liu
Membre du corps professoral de l'Université McGill au Centre du Forum économique mondial pour la quatrième révolution industrielle; Boursier Wilson Chine

Jeff Merritt
Responsable Internet des objets, robotique et villes intelligentes, membre de la direction
Comité, économie mondiale
Forum

À la suite de la pandémie de COVID-19, les technologies portables telles que les trackers de santé et de localisation ont été placées sous les projecteurs du public - suscitant non seulement l'enthousiasme quant à leurs avantages potentiels, mais également le débat sur leurs risques potentiels. Ces dispositifs pourraient-ils aider les autorités de santé publique à mieux prévoir, gérer et éviter de futures éclosions? Comment les employeurs pourraient-ils utiliser les données des appareils portables pour rouvrir des entreprises en toute sécurité? Quelles sont les implications pour la vie privée et l'équité? Comment ces données pourraient-elles être utilisées abusivement ou utilisées à d'autres fins prévues telles que la surveillance publique?

Ces questions sont au cœur des nouveaux efforts du Forum économique mondial, en collaboration avec les autorités de santé publique, les grandes entreprises technologiques et d'autres parties prenantes, pour développer et piloter de nouvelles approches pour le traitement éthique et le partage des données de santé collectées par les appareils portables grand public. [1]

Cet article vise à pousser ces efforts un peu plus loin, en regardant au-delà de la portée du portable dispositifs à l'écosystème plus large des technologies connectées qui se réunissent pour créer «l'internet des corps» (IoB). Comme pour tout domaine de technologie émergente, l'IoB évolue rapidement et son avenir est inconnu. C'est précisément pour cette raison qu'une attention et une réflexion approfondies - non seulement de la part des entreprises, mais aussi du gouvernement, de la société civile et du grand public - sont nécessaires.

Nous sommes au début d'un important dialogue public qui aura des implications majeures pour la santé publique, la sécurité et l'économie mondiale et pourrait également remettre en question notre façon de penser notre corps et ce que signifie être humain.

Ce document ne prétend pas fournir un vue complète de toutes les nombreuses facettes de l'IoB. Cependant, il donne un aperçu de la myriade de problèmes complexes qui peuvent survenir lorsque les mondes cyber et physique se rencontrent. Nous vous invitons à vous joindre à nous dans cet important travail visant à façonner le développement, l'utilisation et l'impact de ces technologies au profit de toute la société.

Résumé

Pour exploiter pleinement le potentiel de l'internet des organes, nous avons besoin de cadres de gouvernance solides et à jour.

> L'Internet des objets (IoT) est de plus en plus s'emmêler avec corps humains.

L'Internet des objets (IoT) est de plus en plus enchevêtré avec le corps humain. Cette émergence et cette expansion rapide de «l'internet des corps» (IoB)[2] - le réseau de corps humains et de données via des capteurs connectés - tout en offrant d'énormes bénéfices sociaux et sanitaires, soulève également de nouveaux défis de gouvernance technologique.

Avec un nombre sans précédent de capteurs attachés, implantés ou ingérés dans le corps humain pour surveiller, analyser et même modifier le corps et le comportement humains, des actions immédiates sont nécessaires pour répondre aux considérations éthiques et juridiques qui accompagnent l'IoB. L'urgence de telles actions est en outre mise au premier plan par la pandémie mondiale de COVID-19, avec de nombreuses technologies et données IoB enrôlées pour la surveillance et le suivi du coronavirus.

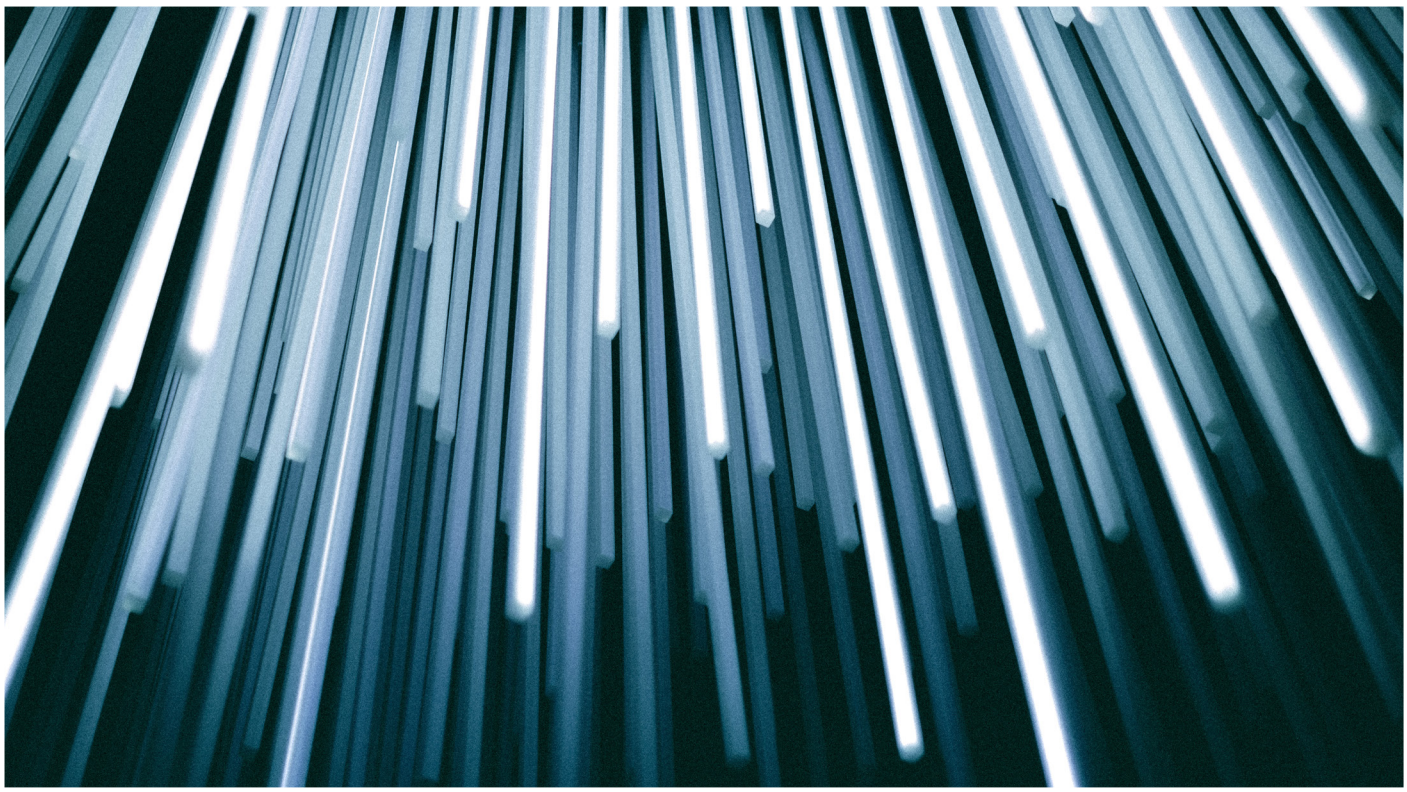
Ce livre blanc comprend deux parties. La première partie présente un aperçu des technologies IoB, ainsi que leurs avantages et leurs risques. Un examen de l'écosystème montre que les technologies IoB sont déployées non seulement dans des scénarios médicaux, mais également dans différents secteurs, de la gestion du fitness et de la santé aux environnements de travail et au divertissement. L'accélération de la convergence des dispositifs grand public et des dispositifs de santé / médicaux montre également que la frontière entre les dispositifs IoB médicaux et non médicaux s'estompe. Cela suggère que de nouvelles stratégies de gouvernance sont nécessaires pour les dispositifs IoB, qui sont traditionnellement soumis à différentes agences et règles de régulation.

Il est à noter que ce livre blanc ne se penchera pas sur les appareils de jeu et de réalité virtuelle (VR) ni sur leurs données. Bien que liés, ces appareils soulèvent des problèmes distincts des appareils de santé et de fitness plus traditionnels.

La deuxième partie examine la gouvernance des données de l'IoB - en se concentrant en particulier sur le paysage réglementaire aux États-Unis, avec une perspective comparative de la réglementation dans l'Union européenne. Cette partie examine les approches réglementaires actuelles des données IoB, ainsi que les défis soulevés par l'écosystème en mutation rapide, en particulier l'adoption à grande échelle des algorithmes de Big Data. Alors que les technologies IoB impliquent également d'autres problèmes tels que les effets physiques des appareils sur les utilisateurs et la responsabilité pour les dommages physiques, cet article se concentre uniquement sur la gouvernance des données générées à partir de l'IoB, en particulier des appareils IoB de santé et de bien-être.

Deux principales conclusions pour les décideurs et les parties prenantes sont mises en évidence. Premièrement, l'adoption à grande échelle de l'IoB et les flux fréquents de données de l'IoB à travers les scénarios et les secteurs nécessitent des cadres de gouvernance solides et cohérents dans les secteurs médical et non médical. C'est particulièrement le cas pour la gouvernance des données IoB car, si les données dérivées cliniquement sont en général strictement réglementées, la réglementation des données générées par les consommateurs et d'autres données non cliniques est souvent, compte tenu de la sensibilité des données, inégale en termes de couverture et force dans tous les secteurs et juridictions; c'est le cas, par exemple, aux États-Unis. Deuxièmement, les approches de gouvernance des données de l'IoB et les lois sur la protection des données nécessitent des mises à jour urgentes pour faire face au risque de confidentialité, d'iniquité et de discrimination engendré par les pratiques courantes d'analyse des mégadonnées.

Nous exhortons donc les parties prenantes de tous les secteurs, industries et zones géographiques à travailler ensemble pour atténuer les risques afin de libérer pleinement le potentiel de l'IoB.



1 Première partie: l'Internet des corps est là

Les progrès récents de l'Internet des objets transforment le corps humain en une nouvelle plateforme technologique.

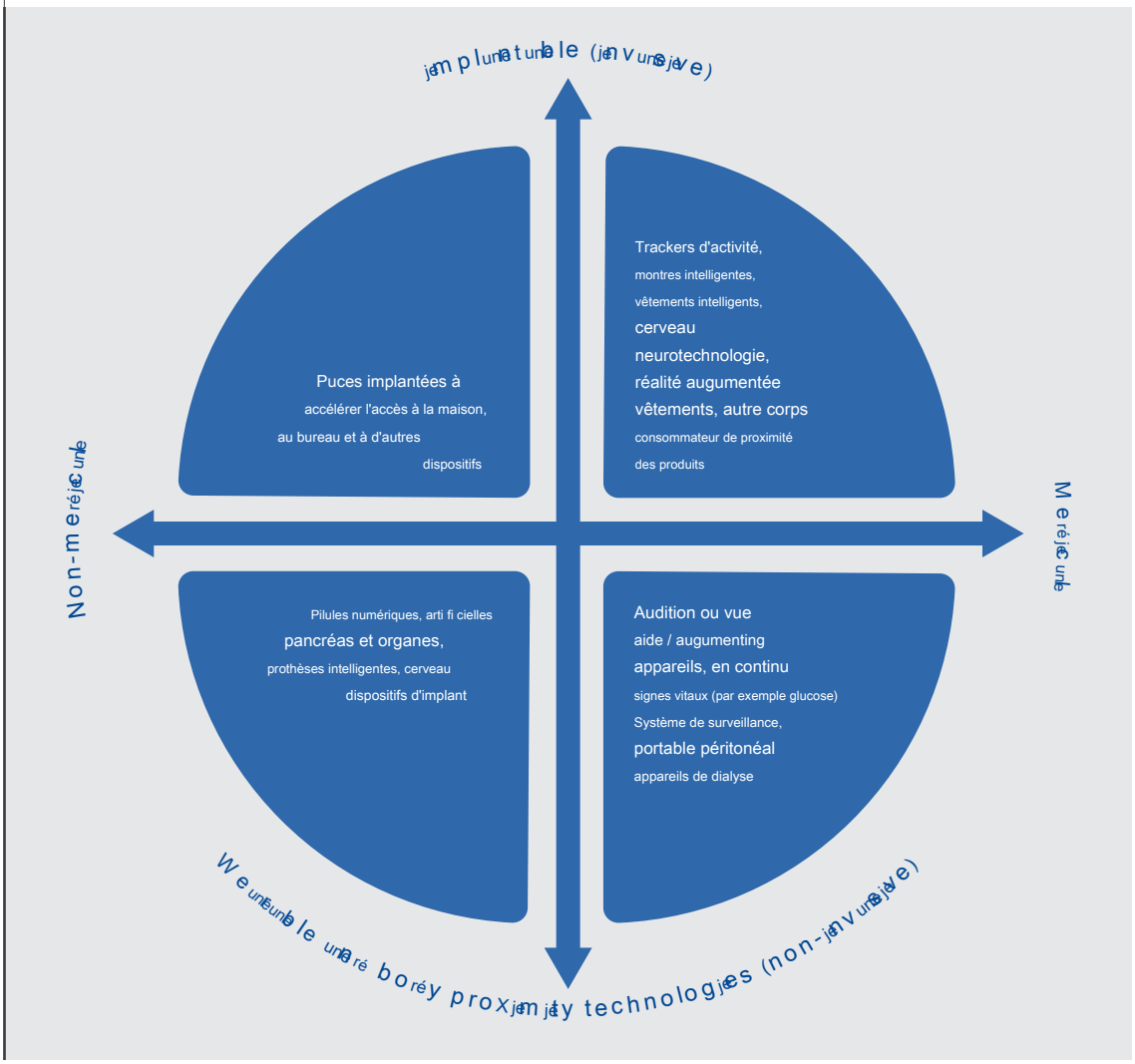
1.1 Gamme et catégories de technologies

Les progrès technologiques récents ont inauguré une nouvelle ère de «l'Internet des corps» (IoB),[3] avec un nombre sans précédent d'appareils et de capteurs connectés fixés ou même implantés et ingérés dans le corps humain. Cela a transformé le corps humain en une plateforme technologique.[4] L'IoB génère d'énormes quantités de données biométriques et comportementales humaines. Cela alimente à son tour la transformation de la recherche en santé et de l'industrie, ainsi que d'autres aspects de la vie sociale, tels que l'adoption de l'IoB dans les environnements de travail, ou la fourniture de nouvelles options de divertissement - le tout avec des innovations remarquables basées sur les données. et les avantages sociaux. Pourtant, l'IoB soulève également de nouveaux défis pour la gouvernance des données qui concernent non seulement la vie privée et l'autonomie individuelles, mais aussi de nouveaux risques de discrimination et de biais dans l'emploi, l'éducation, la finance, l'accès à l'assurance maladie et d'autres domaines importants pour la distribution des ressources sociales.

Généralement, les technologies IoB incluent les dispositifs médicaux,[5] une variété d'appareils de suivi du mode de vie et de la forme physique, d'autres appareils grand public intelligents qui restent à proximité du corps humain et une gamme croissante d'appareils corporels ou intégrés qui sont déployés dans des scénarios d'entreprise, éducatifs et récréatifs. Il convient de noter que les technologies IoB examinées ici sont pour la plupart des «appareils personnels», en ce sens que les appareils développent toujours une relation relativement stable avec le corps individuel de l'utilisateur sur une période de contact régulière et prolongée. Cela exclut donc le type de technologies biométriques installées dans les espaces publics et privés, tels que les systèmes de reconnaissance faciale, les capteurs d'empreintes digitales et les scanners rétiniens, qui se concentrent sur la collecte et le traitement des données d'une grande population ou d'un groupe plutôt que d'individus particuliers.

Comme le montre la figure 1, les technologies IoB peuvent être caractérisées comme non invasives ou moins invasives, en ce sens qu'elles ne devraient pas interférer avec la structure ou une fonction quelconque du corps; ou comme invasif, avec des capteurs passant sous la peau pour être implantés ou faire partie du corps.

FIGURE 1 Exemples de technologies de l'internet des corps



Les technologies invasives comprennent, par exemple, les pilules numériques - une combinaison médicament-dispositif récente développée pour administrer des médicaments encapsulés et surveiller l'observance des médicaments - qui reposent sur des mini-capteurs ingérables à activer dans l'estomac du patient, et qui transmettent ensuite des données aux capteurs, le smartphone du patient et autres portails de données. D'autres exemples d'implantables médicaux intelligents comprennent: un pancréas artificiel connecté à Internet en tant que système d'administration d'insuline automatisé pour les patients diabétiques; et des membres robotiques pour la rééducation des mouvements chez les personnes à mobilité réduite. Ces dernières années, un nombre croissant de personnes ont choisi d'implanter des puces sous leur peau, non à des fins médicales, mais comme choix personnel pour accélérer leur routine quotidienne et pour plus de commodité - accéder à leur domicile, [6] Dans le cadre de la culture du biohacking, les gens ont également cherché à améliorer leur corps avec la technologie implantée, des aimants et des implants de puces RFID aux disques durs miniatures et aux routeurs sans fil. [7]

Parmi les technologies moins invasives, certains appareils restent à la surface du corps humain - on les appelle généralement des appareils portables. Les technologies portables sont un domaine en pleine expansion, avec un marché de 15,74 milliards de dollars en 2015, qui devrait atteindre 51,60 milliards de dollars d'ici 2022. [8] À eux seuls, les patchs électroniques pour la peau, largement adoptés dans les appareils portables médicaux pour la surveillance cardiovasculaire, la gestion du diabète, la détection de la température, de la sueur et des mouvements et d'autres types de surveillance des biomarqueurs, ont généré plus de 7,5 milliards de dollars de revenus en 2018. [9] Les appareils portables non médicaux sont un domaine dynamique, avec des produits et des adoptions allant des trackers personnels de fitness et des smartwatches aux applications d'entreprise. Celles-ci incluent des lunettes et des casques connectés dans les environnements de travail pour le suivi de l'emplacement, la surveillance de la sécurité et l'amélioration des performances au travail; dispositifs neurotechnologiques pour la productivité du travail / apprentissage; et des appareils augmentés et VR pour le divertissement et l'éducation. En plus des technologies implantables et portables, des capteurs intelligents apparaissent de plus en plus dans les produits de consommation ordinaires tels que les peignes, les rasoirs, les brosses à dents, les produits pour la peau, les matelas et autres. Bien qu'ils ne restent pas fixés sur le corps humain à tout moment, ces produits restent à proximité du corps et collectent régulièrement les données biologiques et comportementales des utilisateurs.

Actuellement, les dispositifs IoB médicaux et non médicaux sont souvent soumis à la surveillance de différents organes de gouvernance et d'ensembles distincts de réglementations et de règles juridiques. Aux États-Unis, par exemple, l'approbation avant la mise sur le marché et la surveillance après la mise sur le marché des dispositifs médicaux relèvent du domaine de la Food and Drug Administration (FDA), tandis que les dispositifs non médicaux dans le domaine de la consommation sont principalement supervisés par la Federal Trade Commission. . Pourtant, en termes de scénarios d'utilisation, la division entre les dispositifs médicaux et les dispositifs non médicaux grand public s'estompe. Les fabricants d'appareils portables grand public tels qu'Apple et Fitbit cherchent à étendre leurs produits à des dispositifs de surveillance de la santé certifiés et à faire appel aux assureurs maladie et aux entreprises en tant que clients, tandis que les entreprises de dispositifs médicaux traditionnels construisent également des appareils à utiliser en dehors des établissements médicaux. Les dispositifs IoB sont de plus en plus adoptés dans la division des catégories médicales / non médicales. Les exosquelettes intelligents, par exemple, sont utilisés dans les milieux industriels pour augmenter les performances humaines, mais aussi pour l'aide à la mobilité, la réadaptation et à d'autres fins de santé. Une enquête nationale menée aux États-Unis par Valencell en 2018 a révélé la convergence accélérée des appareils portables grand public et des dispositifs personnels de santé / médicaux. [dix] Cela invite à reconsidérer la frontière entre médical et non médical dans la gouvernance des technologies IoB.

1.2 Avantages sociaux basés sur les données

La variété et la grande quantité de données collectées grâce aux technologies IoB propulsent des transformations dans la recherche et l'industrie en santé, en particulier avec le développement du marché de la santé numérique directement au consommateur. Les technologies IoB ont également été adoptées pour améliorer la sécurité au travail dans les scénarios à haut risque. Quatre des avantages sociaux les plus notables sont détaillés ci-dessous.

1. Permettre le suivi à distance des patients et réduire les infections croisées

La surveillance continue des signes vitaux corporels grâce à des capteurs permet aux prestataires de soins de santé de mieux suivre l'état des patients dans et au-delà des établissements médicaux, depuis les données concernant la pression artérielle, les niveaux d'oxygène, les niveaux de glucose et la fréquence cardiaque jusqu'au sommeil de la personne, les étapes et autres problèmes de santé. facteurs. La surveillance continue est de plus en plus reconnue comme un outil utile pour répondre aux besoins de santé de la population vieillissante dans le monde et des patients atteints d'une maladie chronique. maladie. [11] Récemment, la surveillance à distance a également été utilisée dans la lutte contre l'épidémie de COVID-19. Par exemple, VivaLNK, une start-up de santé connectée basée en Californie, a conçu une solution de surveillance à distance multipatient avec Alibaba pour surveiller en toute sécurité la température du patient, l'électrocardiogramme (ECG), la fréquence cardiaque, la fréquence respiratoire et les mouvements, et réduire le risque d'infection croisée. pour la protection du personnel médical. [12]

2. Améliorer l'engagement des patients et promouvoir un mode de vie sain

Les technologies IoB facilitent l'expansion des soins de santé pour impliquer activement les patients au-delà de l'architecture de la médecine traditionnelle. Un bon exemple est un programme de réadaptation virtuelle que Kaiser Permanente a lancé dans le sud de la Californie en

2019, dans lequel les professionnels de la santé ont surveillé à distance l'exercice et les habitudes de prise de médicaments des patients inscrits en convalescence après des événements cardiaques. Le port de montres intelligentes permet les patients à partager leurs données vitales et leurs activités avec leurs prestataires de soins, qui interagissent régulièrement avec eux. L'amélioration des relations entre les patients et les prestataires de soins et la flexibilité du programme à distance au-delà des cliniques traditionnelles ont amélioré le taux d'achèvement du programme de réadaptation de moins de 50% à 87%, abaissant efficacement les taux de réadmission et réduisant également les coûts médicaux. [13]

3. Faire progresser les soins préventifs et la médecine de précision

Les données fournies par la technologie IoB permettent aux médecins de détecter précocement les maladies et d'offrir des mesures préventives. En outre, le volume et la variété des données peuvent aider à faire progresser la recherche en médecine de précision en reliant les données individuelles sur le mode de vie et l'environnement aux données génétiques et biologiques, fournissant des informations plus approfondies sur les facteurs et les traitements de la maladie. Les appareils portables grand public fournissent de nouveaux types de données et de possibilités dans la recherche scientifique et les essais cliniques. De 2012 à 2017, plus de 500 études publiées ont exploré l'utilisation des appareils Fitbit, avec recherche menée dans une variété de populations et d'environnements d'étude différents. [14] Des sources de données nouvelles et complexes au-delà des contextes cliniques traditionnels peuvent également étendre la recherche de la santé individuelle à la santé de la population pour comprendre comment le comportement humain, les caractéristiques des communautés, les conditions de vie et environnementales, ainsi que les institutions et les politiques, contribuent tous à la santé générale d'une société. groupe. Cela peut potentiellement aider à atténuer les problèmes d'équité existants et potentiels dans l'accès des groupes marginalisés aux ressources de santé.

4. Amélioration de la sécurité au travail

Au-delà des applications de santé, les technologies IoB sont également adoptées dans les lieux de travail dangereux tels que les chantiers de construction, les mines et les usines pour suivre l'emplacement des travailleurs, surveiller les risques environnementaux, réduire l'exposition aux blessures musculo-squelettiques ou autres dommages et atténuer les risques en diffusant des informations à distance. [15] Les données de capteur en temps réel de haute qualité fournissent des conseils aux travailleurs et les conditions de changement rapide, et améliore la surveillance de la sécurité. Les progrès de la neurotechnologie ont également fourni des dispositifs pour le cerveau qui peuvent mesurer la vigilance des pilotes de ligne et des conducteurs afin d'améliorer la sécurité des voyages. Les capteurs biométriques, des casquettes et gilets aux bracelets et aux lunettes, deviennent plus légers et moins chers, et peuvent mesurer le niveau de fatigue des conducteurs et les alerter de quitter la route lorsqu'ils sont somnolents. [16]

1,3 Les risques liés à l'internet des corps

Outre les avantages sociaux et les innovations rendus possibles par les données de l'IoB, de nouveaux risques sont associés à l'utilisation abusive de données contenant des détails intimes sur la santé et les comportements personnels.

Certes, les technologies IoB partagent de nombreuses préoccupations avec l'Internet des objets, telles que la confiance des consommateurs, la sûreté, la sécurité et l'interopérabilité. Plusieurs aspects particulièrement préoccupants sont détaillés ci-dessous.

1. Interopérabilité et exactitude des données

Les problèmes de normalisation des données et d'interopérabilité des technologies présentent des obstacles importants pour combiner et tirer parti de différents types de données provenant de sources variées pour améliorer les soins médicaux et faire progresser la recherche. Avec des millions d'appareils dans l'écosystème de la santé déployés pour surveiller le corps humain, du lit d'hôpital à n'importe quel endroit où les appareils IoB vont avec le corps auquel ils sont attachés, la domination des méthodes de communication propriétaires et fermées entraîne le verrouillage du fournisseur et un manque d'interopérabilité entre ces appareils au niveau de la plateforme et au niveau technique. L'absence d'une plate-forme normalisée pour extraire des flux continus de données à partir de différents appareils limite l'utilisation de ces données pour fournir des informations précieuses, à moins que toutes les sources de données ne soient intrinsèquement issues de périphériques interopérables. De plus en plus, nous constatons une interopérabilité entre les dispositifs portables et les plates-formes grand public, mais cela est plus difficile à garantir lorsqu'il s'agit de combiner ces données avec des données provenant de dossiers médicaux, par exemple. La Health Insurance Portability and Accountability Act (HIPAA) aux États-Unis soutient la portabilité des informations de santé telles que les dossiers médicaux, mais parce que les appareils portables collectent des données qui ne relèvent pas de la HIPAA, il n'y a aucune obligation pour les fabricants d'appareils portables de garantir ce niveau d'interopérabilité du système ou de portabilité des données.

Outre l'interopérabilité, l'exactitude des données est un problème, en particulier avec les appareils de fitness grand public. Actuellement, les dispositifs médicaux et les dispositifs non médicaux sont soumis à différentes normes d'approbation réglementaires et préalables à la mise sur le marché. Cependant, alors que les dispositifs de suivi des consommateurs sont de plus en plus intégrés dans les soins de santé

- par exemple, pour surveiller la fréquence cardiaque et la dépense énergétique chez les patients atteints de maladie cardiovasculaire

- la question de savoir si leurs mesures atteignent un niveau de précision cliniquement acceptable, évaluation des besoins et discrétion. [17] Le remplacement d'appareils de qualité médicale par des appareils grand public peut entraîner des erreurs de diagnostic telles que de fausses alarmes et un traitement excessif. [18] Nous voyons les consommateurs s'appuyer de plus en plus sur les appareils portables pour auto-évaluer leur propre santé en fonction des données des appareils portables, sans la FDA ni la surveillance médicale, et en tant que tels sans conseils.

2. Cybersécurité et confidentialité

Il y a une prise de conscience croissante de la vulnérabilité des dispositifs portables et des appareils IoT médicaux au piratage et aux cyberattaques, qui exposent des vies humaines à des dommages physiques potentiels et à des risques pour la vie privée. À l'échelle mondiale, les violations de la cybersécurité des soins de santé en 2018 représentaient 25% des 750 incidents signalés, plus que tout autre secteur. [19] Le problème n'est pas moins grave pour les appareils grand public. Les chercheurs ont découvert de graves failles de sécurité avec les montres intelligentes pour enfants, que les pirates peuvent utiliser pour suivre les enfants, accéder à l'audio et leur passer des appels téléphoniques. [20]

La confidentialité est l'un des principaux facteurs affectant la confiance des consommateurs et l'adoption des appareils IoB. L'adoption croissante des dispositifs IoB au-delà des installations médicales traditionnelles soulève également de nouvelles préoccupations en matière de sécurité et de confidentialité, tandis que les normes techniques et les politiques ne reflètent pas encore ces nouveaux défis. Par exemple, une carte interactive montrant où se trouvent les personnes qui utilisent des appareils de fitness portables a révélé des informations sur les emplacements et les activités des soldats dans les bases militaires américaines. Pris dans leur ensemble, il s'agit d'informations très sensibles car elles décrivent les mouvements militaires même si les informations d'identification personnelle sont supprimées des données publiées. [21] Au niveau du consommateur, les données de géolocalisation dérivées à partir d'un portable peut indiquer des habitudes de trajet ou d'autres informations qui pourraient être mal utilisées entre de mauvaises mains. Au milieu de l'épidémie mondiale de COVID-19, avec l'obtention de données pour le suivi des coronavirus et l'assouplissement de l'application des données sur la santé aux États-Unis et dans d'autres pays, la confidentialité des données sur la santé a suscité de graves préoccupations. Le (dés) équilibre entre la confidentialité des données et la transparence requise pour faire face à une urgence de santé publique reste un sujet controversé. Par exemple, l'utilisation de données de thermomètres intelligents pour la surveillance de la santé et pour créer une «carte météorologique de la santé aux États-Unis» a soulevé des problèmes de confidentialité alarmants. Certaines sociétés de thermomètres utilisent ces informations personnelles pour commercialiser et vendre les données à des sociétés tierces. [22]

Pour résoudre ces problèmes concernant les appareils portables afin de normaliser l'approche adoptée par les fabricants du monde entier, l'Institut des ingénieurs en électricité et en électronique (IEEE) et son Association de normalisation travaillent avec la FDA, les National Institutes of Health, les universités et l'industrie depuis 2016. Grâce à ces initiatives, l'IEEE et sa communauté ont établi TIPPSS (confiance, identité, confidentialité, protection, sûreté et sécurité) comme principes garantissant la sécurité des patients. [23]

3. Risques de discrimination et d'équité dans l'analyse des données

Les pratiques émergentes liées au traitement des données dérivées des dispositifs IoB signalent des discriminations et préjugés potentiellement alarmants contre les individus. Lorsque ces données générées par l'utilisateur et dérivées biologiquement sont combinées avec des données provenant d'une myriade d'autres sources, telles que les magasins de détail, les sociétés de produits et services de consommation, les services financiers et les institutions gouvernementales pour l'analyse des données, des abus peuvent survenir. L'analyse algorithmique peut être utilisée pour prendre des décisions importantes dans des domaines tels que l'assurance, l'emploi, la finance, l'éducation, la justice pénale, les services sociaux et l'allocation d'autres types de ressources sociales, le tout basé sur des données dérivées de dispositifs IoB. Profilage et regroupement sur la base de données inexactes ou incomplètes, les données indirectes et la génération de données sensibles à partir d'inférences peuvent entraîner des politiques et des prises de décision biaisées qui affectent non seulement les individus, mais aussi les groupes et les populations vulnérables, même si les responsables du traitement des données et les décideurs peuvent parfois ne pas se rendre compte du biais implicite ou du préjudice potentiel. Plusieurs exemples de domaines dans lesquels cette discrimination et ce biais peuvent être observés sont indiqués ci-dessous.

- Polices d'assurance discriminatoires: L'utilisation de données IoB avec des détails minutieux sur les conditions de santé individuelles et les habitudes de vie en assurance pourrait fragmenter le fondement de solidarité de l'assurance et ébranler ses fondements socio-économiques et éthiques. Certains assureurs ont déjà fouillé dans de vastes quantités de données personnelles, allant des adresses de domicile et de propriété, en passant par les niveaux d'éducation, aux données sur le mode de vie telles que les habitudes alimentaires, les activités quotidiennes et les exercices. Les informations sont introduites dans des algorithmes informatiques pour attribuer à chaque individu un score de risque pour les décisions en matière d'assurance maladie, mais aussi dans d'autres types d'assurance, comme l'assurance-vie, l'assurance invalidité et même dans des domaines non directement liés à la santé, comme les prêts financiers. [24] Les données des technologies IoB comprennent souvent des détails précis sur la vie personnelle ainsi que sur la santé physique et mentale. L'utilisation abusive de ces données pourrait conduire à des politiques et des prix d'assurance discriminatoires, rendant plus difficile l'accès des populations marginalisées aux soins de santé de base et à d'autres types d'assurance.

- Discrimination et préjugés en matière d'emploi:
  L'adoption de dispositifs portables et d'appareils IoB dans les programmes de bien-être des employés et dans les scénarios d'emploi crée de nouvelles préoccupations concernant la confidentialité des employés et la surveillance du lieu de travail. Les employeurs utilisant des appareils et des algorithmes pour surveiller et diriger les mouvements, la communication et les comportements des employés, des réglementations relativement faibles dans ce domaine offrent une protection juridique limitée. Cela peut exposer les travailleurs à des risques plus élevés d'utilisation abusive des données et des algorithmes de la boîte noire qui peuvent conduire à des décisions biaisées en matière d'embauche, de promotion et de rétention. [25] Par exemple, des algorithmes d'embauche et les technologies prédictives reproduisent les biais institutionnels et historiques, mais ces biais sont moins faciles à détecter en raison du manque de transparence des algorithmes et des sources et de la qualité des données utilisées pour cette formation d'algorithmes. [26] Les risques accrus d'intrusion et d'injustice dans la vie privée ont déjà suscité l'opposition des employés, des syndicats et des militants. [27] En 2018, les enseignants de Virginie-Occidentale se sont mis en grève pour exiger la suppression d'un programme de bien-être au travail qui avait été critiqué pour avoir pénalisé les membres pour ne pas avoir obtenu des niveaux «acceptables» sur les mesures biométriques. [28]

  Les travailleurs des entrepôts UPS, McDonald's et Amazon ont également protesté contre le stress au travail exacerbé et la précarité imposés par la direction grâce à des traqueurs intensifs de collecte de données, et ont demandé de nouvelles règles concernant les employeurs qui utilisent les données de suivi pour discipliner les employés. [29]

- Politique publique qui crée et / ou renforce les inégalités sociales: Les décideurs utilisent de plus en plus de nouvelles sources de données et d'analyses de données pour la prise de décisions dans les politiques publiques telles que la santé, les interventions en cas de catastrophe, la conception urbaine, la sécurité nationale, le développement économique et d'autres domaines. Biais potentiel

  dans les types et la qualité des données et des algorithmes peuvent créer intentionnellement ou non
  et renforcer les inégalités sociales, en limitant l'accès de certains groupes sociaux à la santé et à d'autres ressources publiques. De nouvelles sources de données provenant de téléphones mobiles et d'appareils IoB, par exemple, ont été adoptées pour suivre et prévoir l'épidémie et la transmission de maladies. Pourtant, lorsqu'elles sont déployées sans tenir compte des biais potentiels des données et des algorithmes, il existe un risque que les données retirent une épidémie de son contexte politique et sociétal et, en particulier, affectent la vie des populations vulnérables. Dans le cas de l'épidémie d'Ebola de 2014, par exemple, de nombreuses organisations humanitaires actives en Afrique ont encouragé les gouvernements, les fondations caritatives,

  entreprises technologiques et réseaux mobiles pour partager des données. Mais des études montrent qu'ils ne disposaient pas des capacités de modélisation des données, des normes professionnelles de mise en œuvre de la technologie et de la capacité d'application pour définir ou protéger l'intérêt public, ce qui a entraîné la violation des droits humains fondamentaux et aggravé le fossé des inégalités en termes d'accès aux ressources d'assistance en cas de catastrophe. [30]

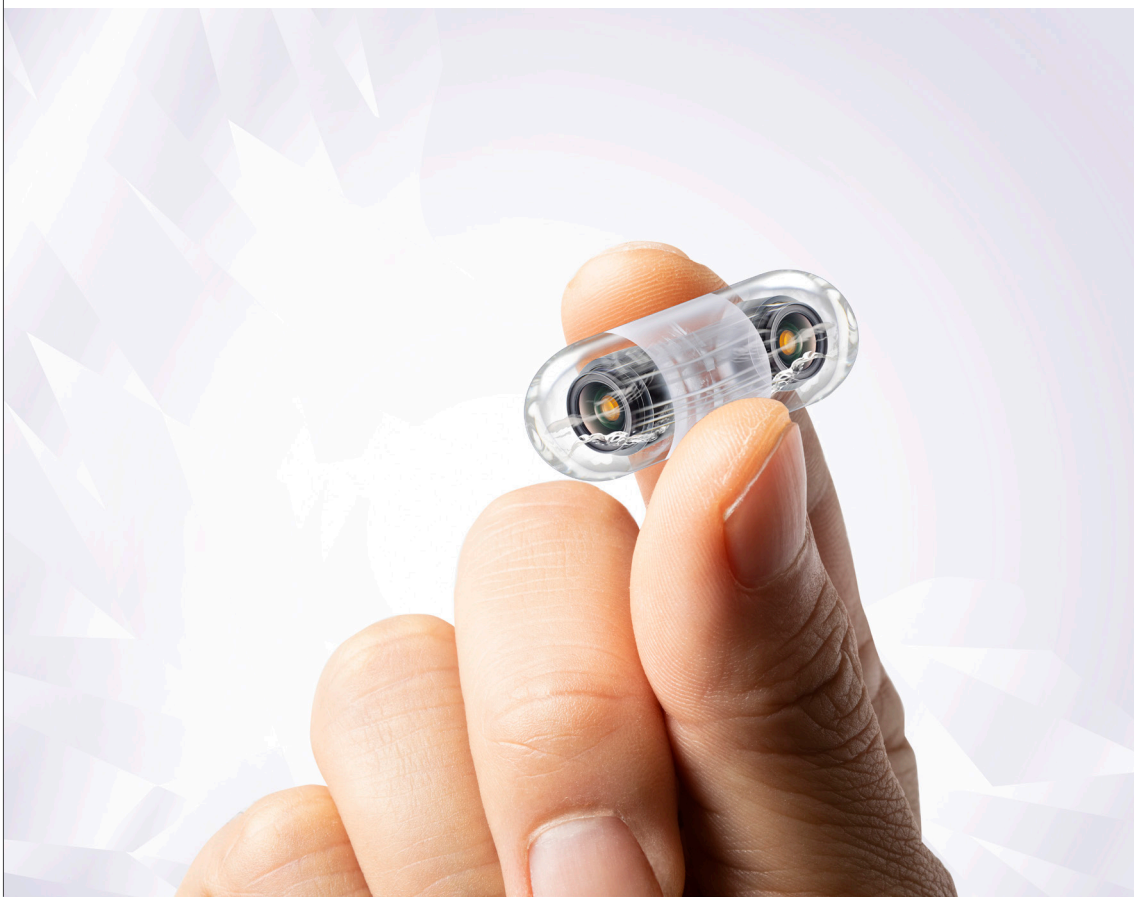
L'adoption de l'analyse des données dans la prise de décision implique un volume, une vitesse et une variété de données sans précédent, parmi lesquels les données des technologies IoB sont combinées avec celles d'autres sources à des fins de référence croisée. Cela suggère que la collecte et l'utilisation des données de l'IoB vont souvent au-delà du secteur de la santé; et d'autre part, des données qui ne sont pas directement liées à la santé,

telles que les données des médias sociaux, peuvent également être utilisées pour générer des analyses relatives à la santé individuelle et collective. Ces pratiques émergentes et ces risques potentiels soulèvent de nouveaux défis dans la gestion des données générées par la gamme croissante des réseaux IoB. Il est déjà difficile de protéger les droits des données et d'assurer la transparence et l'équité à l'ère du big data, et les défis spécifiques que les technologies IoB créent dans cet espace signifient qu'elles doivent être considérées comme faisant partie de ce débat.

Comme nous le verrons dans la section suivante, alors que les données cliniques sont, en général, soumises à une réglementation stricte, la gouvernance des données du mode de vie basé sur la santé et d'autres dispositifs non médicaux est plus inégale en raison de la divergence des réglementations sur les données entre les secteurs et sous juridictions différentes. Il est suggéré que les lois régissant la collecte de données médicales sont largement insuffisantes pour faire face aux risques de sécurité, de confidentialité et de discrimination découlant du traitement des données IoB.

2 Deuxième partie: la gouvernance des données de l'internet des corps

Les réglementations actuelles abordent certains des nombreux risques introduits par les données IoB, mais pas tous.



Bien que la fabrication et la sécurité des appareils IoB puissent être soumises à différentes agences gouvernementales et à des règles connexes (telles que les réglementations et directives de la Federal Communication Commission [FCC] pour la fabrication d'appareils IoT aux États-Unis), l'accent est mis ici sur la collecte, le transfert et utilisation des données IoB, en particulier les risques de discrimination qui viennent avec l'analyse des données. Comme discuté, l'adoption des technologies IoB ne se limite pas à l'espace des applications médicales mais couvre différents secteurs. Cela est encore compliqué par la pratique de l'analyse des données, qui génère constamment de nouvelles données en combinant et en analysant différentes sources de données, quelle que soit leur origine.

2,1 Paysage réglementaire des données aux États-Unis et dans l'UE

> Dans les deux Les États-Unis et l'UE, il reste un écart entre anti-discrimination lois et nouveau risque de la discrimination résultant de basé sur les données inférences, profilage et le regroupement.

Cette section examine le paysage réglementaire des données IoB aux États-Unis, avec une comparaison avec l'Union européenne. Les réglementations relatives aux données IoB pertinentes aux États-Unis sont sectorielles, avec des lois distinctes pour différents types d'informations, d'utilisateurs et de situations. La navigation est compliquée pour les contrôleurs de données et les utilisateurs, et la couverture et la force de la protection des données peuvent diverger considérablement d'un secteur à l'autre et selon les réglementations nationales et locales. Alors que les données médicales sont souvent considérées comme sensibles et donc strictement réglementées, les données non médicales des appareils grand public sont pas toujours soumis à un niveau de protection équivalent, même en ce qui concerne les données physiologiques, telles que celles provenant d'appareils de fitness. En Europe, par comparaison, le règlement général sur la protection des données (RGPD) est un règlement sur les données non sectoriel et technologiquement neutre qui fournit des lignes directrices pour les procédures de collecte et de traitement des données personnelles. Aux États-Unis et dans l'UE, il subsiste un fossé entre les lois anti-discrimination et le nouveau risque de discrimination découlant des inférences, du profilage et du regroupement basés sur les données.

Réglementations existantes aux États-Unis

Les États-Unis n'ont pas de loi complète sur la protection des données réglementant tous les aspects de la confidentialité ou de la sécurité des informations. Les données générées à partir de la technologie IoB pourraient être soumises à trois corps de loi et de réglementation: lois et règlements fédéraux spécifiques au secteur; lois anti-discrimination au niveau fédéral; et les lois et réglementations au niveau de l'État, du comté et au niveau local.

1. Lois et normes fédérales pertinentes aux États-Unis

- Loi sur la portabilité et la responsabilité de l'assurance maladie (HIPAA): La HIPAA, complétée par la loi de 2009 sur les technologies de l'information sur la santé pour la santé économique et clinique (loi HITECH), réglemente l'utilisation et la divulgation des «informations de santé protégées» (PHI) par les entités couvertes. Les entités couvertes comprennent les plans de santé, les prestataires de soins de santé, les chambres de compensation des soins de santé et leurs associés commerciaux. La HIPAA fournit également des conseils concernant deux méthodes qui peuvent être utilisées pour satisfaire à la norme de désidentification de la règle de confidentialité: la détermination d'experts et la sphère de sécurité.[31] La règle de confidentialité de HIPAA ne s'applique pas aux données non identifiées, ni aux données au-delà de PHI traitées par entités couvertes.

- Loi sur la Commission fédérale du commerce (FTC):
  La loi FTC, sssss appliquée par la Federal Trade Commission, interdit aux entreprises de se livrer à des actes ou pratiques trompeurs ou déloyaux, y compris à ne pas se conformer à la politique de confidentialité d'une entité, entre autres.[32]
  Cela fait de la loi FTC la principale loi fédérale applicable aux pratiques de confidentialité et de sécurité entourant les appareils IoB grand public.

- Les principes de pratiques équitables en matière d'information (FIPP): Administrés par la FTC, les FIPP guident l'interprétation de la protection des données qui caractérise l'approche sectorielle de la législation américaine sur la protection de la vie privée. Ce qui était à l'origine de larges principes consensuels en tant que normes a évolué pour devenir un ensemble de règles plus prescrit appliqué dans différents contextes de protection de la vie privée. Ils sont à la base de l'approche du groupe social et du contexte, allant des données médicales (HIPAA) et financières (Gramm-Leach-Bliley Act [GLBA]) aux droits des enfants (Children's Online Privacy Protection Act [COPPA]), aux étudiants (Family Educational Loi sur les droits et la vie privée [FERPA]), les consommateurs (par exemple, Loi sur les consommateurs de téléphone [TCPA]) et la vie privée du conducteur (Loi sur la protection de la confidentialité du conducteur [DPPA]).

- Loi Gramm-Leach-Bliley (GLBA): La GLBA réglemente les informations financières personnellement identifiables qui sont fournies par, résultent ou sont autrement obtenues en relation avec les consommateurs et les clients qui obtiennent des services financiers, y compris les fournisseurs d'assurance. Il limite la divulgation des renseignements personnels non publics recueillis par une institution financière. Il ne restreint pas l'utilisation des informations personnelles ou des analyses de données volumineuses pour personnaliser les contrats d'assurance.[33]

- Le Fair Credit Reporting Act (FCRA): La FCRA réglemente toute «agence d'information sur les consommateurs» (ARC) qui fournit un «rapport sur le consommateur» à utiliser principalement pour aider à établir l'admissibilité d'un consommateur au crédit, lorsque le rapport porte sur la solvabilité, la solvabilité, le caractère, la réputation générale de la personne, caractéristiques personnelles, modèle de vie, etc.

- La politique fédérale de protection des sujets de recherche (règle commune): Commun

La règle s'applique à la recherche impliquant la collecte ou l'étude de données, documents, enregistrements, échantillons pathologiques ou échantillons diagnostiques existants, mais les informations anonymes ou désidentifiées sont expressément exemptées de la réglementation.

- En plus de ceux-ci, d'autres réglementations spécifiques, telles que la Family Educational Rights and Privacy Act (FERPA), la COPPA et les règles de confidentialité des consommateurs à large bande de la FCC, peuvent être pertinentes pour
le partage et l'utilisation des données liées à l'IoB dans des contextes spécifiques variés.

2. Lois anti-discrimination au niveau fédéral aux États-Unis

> Aux États-Unis, le Loi sur les droits civils de 1964 interdit la discrimination basé sur l'individu caractéristiques comme la race, religion ou sexe.

En vertu de la Constitution américaine, une caractéristique commune d'un groupe, comme la couleur de la peau, le sexe ou l'orientation sexuelle, ne doit pas constituer la base d'un traitement inégal. Le Civil Rights Act de 1964 interdit la discrimination fondée sur des caractéristiques individuelles telles que la race, la religion ou le sexe. Les lois pertinentes concernant la discrimination à l'égard des personnes présentant certaines caractéristiques sont les suivantes:

- American with Disabilities Act (ADA): L'Americans with Disabilities Act de 1990 a été promulguée pour éliminer les barrières discriminatoires à l'encontre des personnes handicapées qualifiées, des personnes ayant des antécédents de handicap et des personnes perçues comme ayant un handicap. Pourtant, il n'atteint pas les personnes qui sont actuellement en bonne santé mais qui sont perçues comme étant à haut risque de tomber malades à l'avenir, et par conséquent, il ne réglemente pas un certain nombre de parties, telles que les employeurs, les institutions financières, les commerçants et les établissements d'enseignement, qui sont susceptibles de s'intéresser aux données prédictives sur la santé des individus. [34]

- Loi sur la protection des patients et les soins abordables (ACA): L'ACA vise à garantir la non-discrimination dans le cadre des programmes financés dans le cadre de l'ACA. Elle interdit la discrimination fondée sur la race, la couleur, l'origine nationale, le sexe, l'âge ou le handicap dans certains programmes et activités de santé. En interprétant les lois sous-jacentes sur la race et le sexe de l'ACA, les tribunaux ont estimé qu'elles interdisent uniquement la discrimination directe mais non indirecte.

- Loi sur la non-discrimination des informations génétiques (GINA): Le GINA protège les résidents américains de la discrimination génétique dans la couverture de l'assurance maladie et les contextes d'emploi. Cependant, il exclut d'autres formes d'assurance telles que l'assurance-vie, l'assurance soins de longue durée et l'assurance invalidité. Il ne traite pas des risques de discrimination dans l'éducation, la finance (comme les prêts hypothécaires) ou le logement.

D'autres lois et réglementations anti-discrimination, telles que la loi sur la discrimination fondée sur l'âge dans l'emploi et la loi sur la discrimination liée à la grossesse, peuvent être pertinentes dans des contextes spécifiques.

3. Au niveau des États et autres lois et réglementations locales aux États-Unis

Les lois et réglementations au niveau des États, des comtés et des municipalités, ainsi que d'autres réglementations spécifiques au secteur, sont applicables dans les juridictions respectives. Les exemples pertinents incluent le California Consumer Privacy Act (CCPA), l'Illinois Biometric Privacy Act (BIPA) et le New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), entre autres. [35] La CCPA est la première loi aux États-Unis à mettre en place un ensemble complet de règles concernant les données des consommateurs et s'applique à toute entreprise qui opère en Californie et qui satisfait à l'un des seuils définis. La loi SHIELD exige que toute personne

ou une entreprise détenant ou autorisant des données informatisées comprenant les informations privées d'un résident de New York («entreprise couverte») pour mettre en œuvre et maintenir des mesures de protection raisonnables pour protéger la sécurité, la confidentialité et l'intégrité des informations privées. Le BIPA fait partie des lois sur la confidentialité biométrique des États les plus complètes, et

permet aux individus d'intenter des poursuites pour violation de leur vie privée même si les individus ne subissent aucun préjudice réel. Mais il existe également des lois étatiques sur la protection de la vie privée qui ont échoué. Par exemple, au début de 2020, pour la deuxième année consécutive, la législation sur la confidentialité des données a échoué dans l'État de Washington. Il existe également d'autres réglementations de comté et de ville liées aux données biométriques. Par exemple, bien que les systèmes de reconnaissance faciale installés dans les espaces publics soient exclus du champ d'application des technologies IoB examinées dans ce livre blanc, les interdictions de reconnaissance faciale de San Francisco et Boston démontrent des approches locales de régulation des données biométriques. En général, la gouvernance de l'Etat et au niveau local de l'IoB et des données biométriques est dynamique et en constante évolution.

En plus des réglementations gouvernementales, des groupes commerciaux et des organismes à but non lucratif soutenus par l'industrie, tels que la Consumer Technology Association et

the Future of Privacy Forum, ont élaboré un certain nombre de lignes directrices, de codes de conduite, de principes et de méthodologies pour la protection de la vie privée et la réglementation des données

du bien-être des consommateurs et des produits portables.[36]
Ces programmes offrent un patchwork d'autorégulations de l'industrie.

TABLEAU 1 Risques et lacunes dans les exemples pertinents de politiques aux États-Unis

Problèmes et risques	Exemples de politiques aux données IoB	Lacunes majeures	Exemples de réglementations locales
Portée limitée de "information sur la santé"	HIPAA	Pas de couverture sur les données du direct au consommateur dispositifs médicaux et appareils grand public qui ne sont pas traités par des identités couvertes; non couverture sur les inférences sur les informations de santé	Californie médicale Loi sur la protection des renseignements personnels (CMIA) étend la santé protection des informations devoirs envers les fournisseurs de logiciel, matériel et services en ligne
Risques de discrimination FCRA; GLBA; GINA en finance et Assurance	(assurance santé)	Adressage irrégulier l'utilisation de la santé et de la santé information dans la vie assurance, à long terme assurance soins et autres types d'assurances; quelques mesures à prendre les risques de l'analyse du Big Data	CCPA (n'impose aucune obligation légale organismes gouvernementaux, mais peut être pertinent lorsqu'il s'agit d'impliquer divulgation sur le tiers des soirées) BIPA (réglemente comment les entités privées collectent, utiliser et partager des informations biométriques) SHIELD Act, etc.
Risques de discrimination employé	Constitutionnel droits (s'appliquent à fédéral et état Gouvernements); GINA; ADA; la grossesse Loi sur la discrimination	Quelques mesures pour traiter les données prédictives de la Loi sur la protection des renseignements sur la santé; varie entre publique et privée secteurs; exemption fait à l'employeur bien-être offert programme dans lequel un employé volontairement participe	Californie médicale (CMIA) étend la santé protection des informations devoirs envers les fournisseurs de logiciel, matériel et services en ligne
Risques de discrimination en politique publique	Quatrième amendement à la Constitution américaine du paysage compliqué (interdit l'accès au gouvernement personnel recherches déraisonnables et saisies, y compris les deux recherches physiques et recherche des informations personnelles via écoutes téléphoniques et accès aux archives de l'entreprise)	information pour la loi exécution et la sécurité nationale	

4. Perspective de l'Union européenne et RGPD

Les droits fondamentaux de protection des données à caractère personnel et le droit à la vie privée et familiale, au domicile et aux communications sont inscrits dans la Charte des droits fondamentaux de l'UE.[37] Les lois de l'UE sur la protection des données et la vie privée reposent sur la distinction entre les données personnelles et les données non personnelles, avec une protection de niveau supérieur pour des catégories spéciales de données personnelles, telles que les données de santé.

Le RGPD de l'UE, en vigueur depuis 2018, s'applique à la collecte, au transfert et au traitement des données personnelles. Il est complété par une directive ePrivacy distincte[38] qui garantit la confidentialité des données lors de la transmission, par exemple sur l'infrastructure de réseau entre deux parties, et peut inclure la protection de la confidentialité des métadonnées ainsi que des données personnelles.

Les dispositions vitales pertinentes pour les données de l'IoB sont les suivantes:

- Principes de protection des données: Le RGPD présente un ensemble de principes à suivre lors de la collecte, du traitement et du stockage des données personnelles, y compris: la limitation des finalités, la minimisation des données, la limitation du stockage, l'exactitude, l'intégrité et la confidentialité (sécurité), la responsabilité et la légalité, l'équité et la transparence. Cependant, la définition vague de «l'équité» compromet une protection efficace contre le risque de discrimination résultant de l'analyse des données. En outre, la base juridique de la collecte de données personnelles auprès d'une personne doit être déterminée par le sous-traitant. Parfois, cela repose sur le consentement et

  il se fonde parfois sur un intérêt légitime ou sur l'exécution d'un contrat, pour ne citer que trois possibilités au titre de l'article 6.

- «Données relatives à la santé» en tant que catégorie spéciale de données: Les «données relatives à la santé» sont définies dans le RGPD comme «des données personnelles liées à la santé physique ou mentale d'un individu, y compris la fourniture de services de santé, qui révèlent des informations sur son état de santé».[39] Distinctes de la définition HIPAA des informations personnelles sur la santé, les données sur le mode de vie et le bien-être des appareils grand public doivent être considérées comme des données de santé,

  surtout lorsqu'elle est traitée dans le but de surveiller la santé ou le bien-être d'un individu. Outre les motifs légitimes de traitement des données à caractère personnel énumérés à l'article 6, l'article 9 énumère les conditions de traitement des données de catégorie particulière, qui comprennent: le consentement explicite de la personne concernée pour l'évaluation de la capacité de travail du salarié; raisons d'intérêt public substantiel; santé publique; recherche etc.

- Droit de contester la prise de décision individuelle automatisée: L'article 22 énonce le droit de la personne concernée «de ne pas être soumise à une décision fondée uniquement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques la concernant ou l'affecte de manière significative de manière similaire»,[40] et les exceptions à ces règles. En outre, les décisions automatisées ne doivent pas être fondées sur des catégories particulières de données.

Au-delà du RGPD, le droit européen de non-discrimination, tant le droit primaire (la charte des droits fondamentaux de l'UE) que le droit secondaire, peuvent être pertinents lorsqu'il s'agit de l'utilisation des données pour des décisions discriminatoires dans des domaines tels que l'emploi, le système de protection sociale et l'accès aux biens et services. Parmi les exemples de droit secondaire de non-discrimination, citons la directive sur l'égalité raciale (2000/43 / CE), la directive sur l'égalité entre les hommes et les femmes (refonte) (2006/54 / CE) 94 et la directive sur l'accès des femmes aux biens et services (2004/113 / CE) 95, mais il existe une divergence sectorielle.[41] Alors que la Charte des droits fondamentaux de l'Union européenne et d'autres lois visent la mise en œuvre des principes d'égalité de traitement, des exceptions ont été créées, lorsque, par exemple, dans les services financiers, la segmentation de la clientèle fondée sur des facteurs actuariels était exclue du champ d'application de la loi existante sur la discrimination. . En outre, alors que l'utilisation de l'identité pour la segmentation de la clientèle a été déclarée illégale par la Cour de justice européenne, l'utilisation de données sur le mode de vie pour générer des inférences et des scores de risque soulève de nouveaux défis pour la transparence et l'équité. Dans un rapport publié en 2019, Finance Watch identifie les données des appareils de santé connectés comme un domaine à haut risque pour les polices d'assurance discriminatoires et l'exclusion sociale.[42]

2.2 Nouveaux défis de gouvernance à l'ère du big data

Les problèmes soulevés par l'expansion des technologies IoB et les lacunes du paysage réglementaire représentent des préoccupations beaucoup plus larges concernant les risques liés à la confidentialité des données et droits ainsi que de nouveaux défis pour la protection des données à l'ère de l'analyse des mégadonnées. Six de ces défis urgents en matière de gouvernance sont décrits ci-dessous.

1. Définition des «données sur la santé»

Les technologies IoB ont généré des volumes élevés de données physiologiques et biométriques qui dépassent de loin les définitions traditionnelles des informations sur la santé, qui se réfèrent principalement aux dossiers médicaux des patients et aux échantillons biologiques obtenus dans des contextes cliniques. Les appareils portables grand public et les technologies de proximité du corps se sont avérés précieux pour capturer des données sur la santé et le bien-être au-delà des installations médicales. Il existe également d'autres types de données, telles que les registres de vente au détail et les données des médias sociaux, qui pourraient être utilisées pour déduire des détails sur les personnes physiques et santé mentale.[43] Lors d'un incident largement rapporté, la chaîne de vente au détail Target a découvert qu'une adolescente était enceinte avant que ses parents ne le sachent grâce à l'analyse de ses registres d'achats.[44] Alors que les réglementations sur les données de santé telles que la HIPAA se concentrent traditionnellement sur les informations sur les patients dans l'architecture de santé traditionnelle, les limites floues des données de santé rendent inadéquate l'approche de la réglementation des données spécifique au dépositaire (où et comment les données sont créées) pour traiter les flux fréquents de données entre les secteurs. et contextes.

2. Équilibrage de l'utilité des données et des principes de protection des données existants

La prolifération des technologies IoB, ainsi que le volume, la vitesse et la variété des données impliquées dans l'analyse et la modélisation prédictive, est l'aspect le plus important et le plus puissant du Big Data. Les principes de base de la protection des données tels que la «minimisation des données» et la «limitation des finalités» peuvent aller à l'encontre des pratiques de Big Data qui nécessitent des quantités massives de données pour la formation des algorithmes, et impliquent souvent la réutilisation et l'utilisation combinatoire des données.

Dans la pratique, il est également difficile de prévoir les finalités du traitement et de l'utilisation secondaire des données. Ces principes, qui ont guidé les politiques de confidentialité et de protection des données en Europe et aux États-Unis, sont largement dérivés des principes de pratique équitable de l'information (FIPP) élaborés dans les années 1970. Ces principes doivent être réévalués et mis à jour pour s'adapter aux nouvelles pratiques de l'analyse du Big Data.

3. Gérer les informations personnellement identifiables (PII) et les données personnelles

Étant donné que les règles de protection des données se concentrent historiquement sur les informations personnellement identifiables (PII) et les données personnelles, le seuil d'identifiabilité et la possibilité de réidentification deviennent cruciaux pour définir les risques pour la vie privée. Les exigences existantes en matière de désidentification, telles que la disposition HIPAA Safe Harbor qui exige la suppression de 18 types d'identificateurs, ont été critiquées pour avoir entravé les activités de recherche sans offrir une protection efficace de la vie privée.[45] Une utilisation efficace des données pour la recherche en santé peut nécessiter de relier les données multisourcées de sorte que les données décrivant un individu situé dans une source soient liées à celles d'autres sources. D'une part, l'approche «taille unique» de la désidentification peut affecter l'intégrité et l'utilité des données dans la recherche, et d'autre part, elle a été s'est avérée insuffisante pour protéger la vie privée, non seulement parce que la désidentification ne fonctionne pas pour les données génomiques, mais aussi parce que les données désidentifiées pourraient potentiellement être réidentifiées par corrélation croisée d'éléments de données avec des ensembles de données externes, tels que les registres d'inscription des électeurs, les bases de données disponibles dans le commerce et d'autres sources.[46] On estime qu'entre 63% et 87% de la population des États-Unis pourraient être identifiés de manière unique en utilisant uniquement leur sexe, leur code postal et leur date de naissance.[47] Pourtant, la classification des données qui répondent à la norme de désidentification en tant que données non personnelles les placera au-delà des règles de confidentialité des données HIPPA, même si, en réalité, les limites des informations personnelles identifiables deviennent fluides dans l'environnement du Big Data.

4. Catégorisation des "données sensibles"

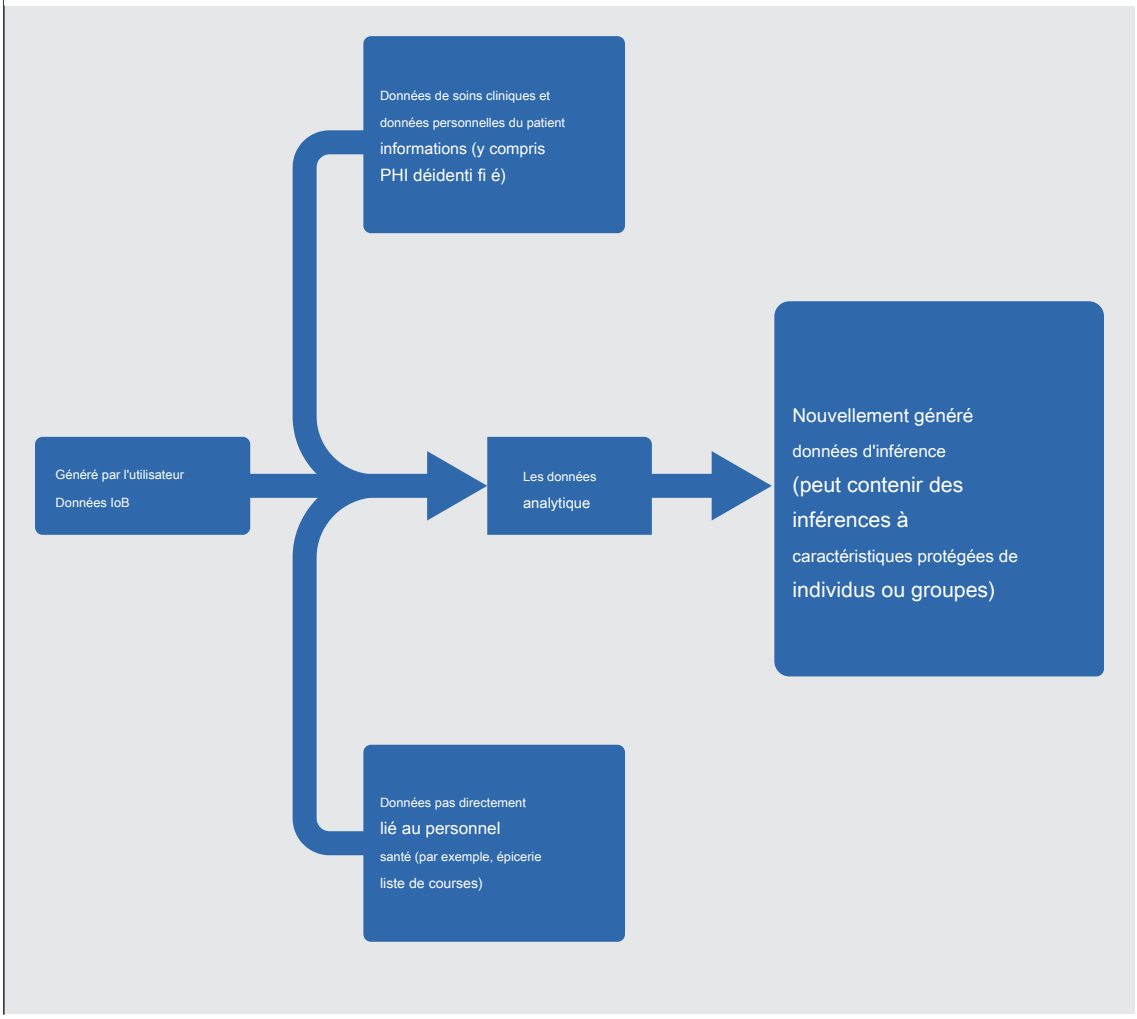
Certaines données sont plus sensibles que d'autres, et même les métadonnées non personnelles peuvent être de nature sensible. Avec l'analyse des mégadonnées, des inférences sur l'état de santé d'une personne peuvent être tirées de données de santé indirectement liées; Les données sur la santé et le comportement des technologies IoB peuvent également être utilisées pour faire des inférences à des fins de prévisions et de prise de décision dans des domaines tels que l'assurance, l'emploi et la finance. Les agents publics et privés peuvent tirer des «inférences à haut risque», c'est-à-dire des inférences tirées d'analyses de mégadonnées qui portent atteinte à la vie privée ou ont une faible vérifiabilité, pour les revendications et les décisions qui peuvent nuire aux intérêts des individus et des groupes.[48] Le profilage et l'analyse inférentielle peuvent générer des informations sensibles telles que l'origine raciale ou ethnique à partir de données classées comme informations non sensibles par les réglementations existantes, telles que par code postal. Par exemple, le profilage d'affinité

- le regroupement des personnes en fonction de leurs caractéristiques inférées ou corrélées plutôt que de leurs caractéristiques personnelles connues - augmente le risque de ce que Sandra, experte en protection des données de l'Oxford Internet Institute

Wachter appelle «discrimination par association», une situation dans laquelle une personne est traitée beaucoup moins bien que les autres en raison de sa relation présumée ou de son association avec un groupe protégé. Un tel profilage d'affinité génère donc des inférences sensibles concernant l'appartenance ethnique, l'orientation sexuelle et d'autres traits personnels de la personne, même si ce profilage n'est pas obtenu par le traitement de données sensibles protégées (par exemple des catégories spéciales de données dans le RGPD).[49] En outre, le degré de sensibilité dépend également de l'objectif et du contexte de l'utilisation des données. Par exemple, les informations sur l'âge d'une personne peuvent ne pas être considérées comme sensibles mais pourraient être utilisées contre elle dans des décisions importantes en matière d'assurance et d'embauche. Cette

n'est pas de nier que les données médicales et autres données IoB directement liées aux fonctionnalités protégées sont sensibles, mais d'attirer l'attention: l'analyse inférentielle des mégadonnées rend inadéquates les mesures réglementaires qui reposent uniquement sur des catégories limitées et statiques de données sensibles / non sensibles au moment de leur collecte et avant leur traitement.

FIGURE 2 : Risques d'inférences sensibles



5. «Autogestion de la confidentialité» et consentement

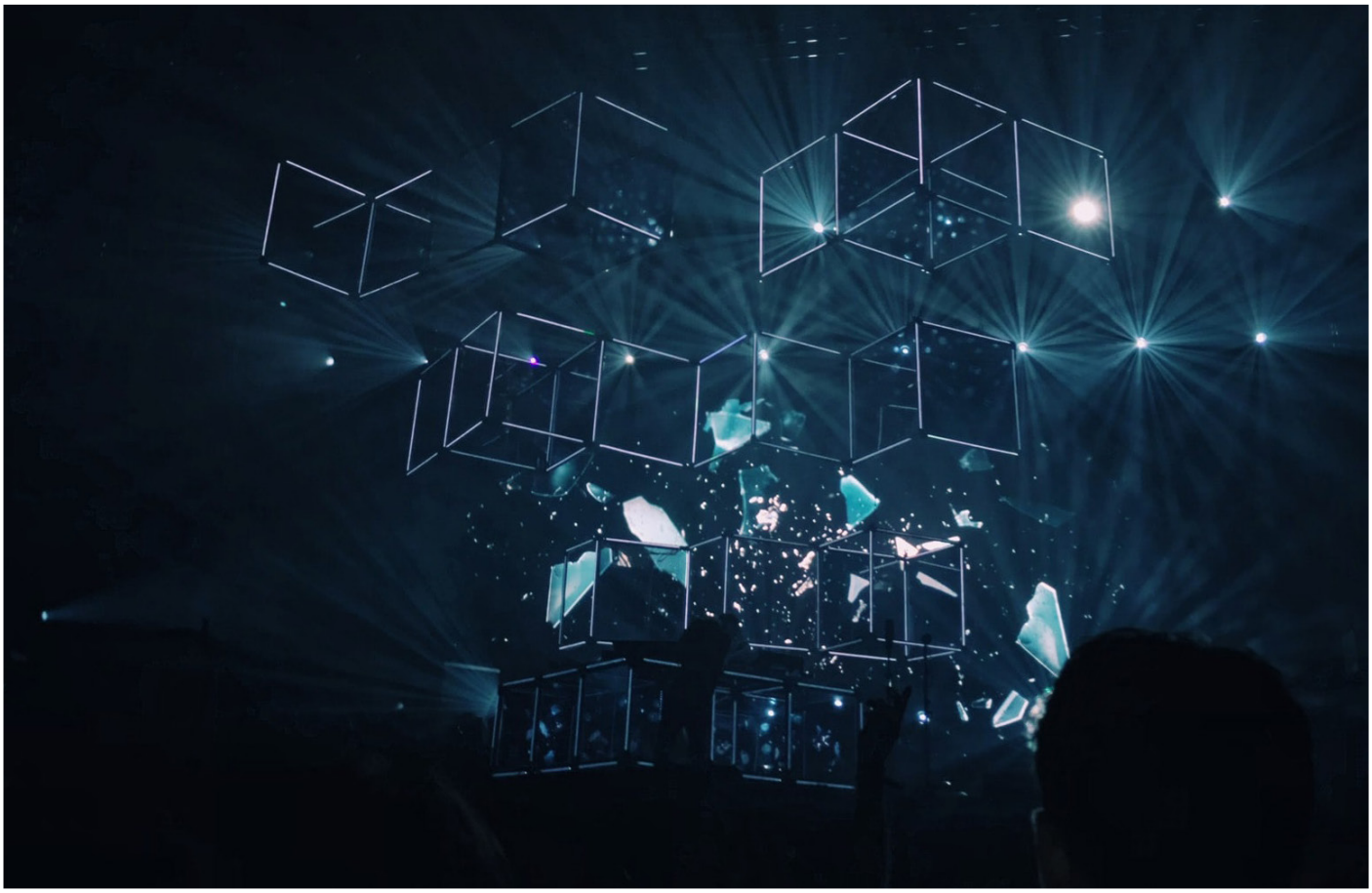
Il est de plus en plus difficile pour les personnes concernées de retracer quelles données sont collectées et comment leurs données sont utilisées en raison du caractère mutable des données traitées et de l'opacité des codes algorithmiques. Le mécanisme de «notification et consentement» ne traite ni de l'opacité des algorithmes ni de la modélisation prédictive,[50] ni les asymétries de connaissances et de pouvoir entre les personnes concernées et les responsables du traitement. Par conséquent, le modèle de notification et de consentement, qui met l'accent sur «l'autogestion de la vie privée» des individus, relève souvent de la formalité juridique.

en raison du langage délibérément obscur et de l'impossibilité de tracer et de gérer des flux de données fréquents et de l'imprévisibilité des résultats du traitement. En outre, les environnements de Big Data interconnectés peuvent présenter une «interdépendance de la vie privée», des situations dans lesquelles la vie privée d'une personne est affectée par la décision d'autrui.[51] Les données génétiques, qui sont partiellement partagées avec les membres de la famille, et la révélation que les données génétiques d'une personne peuvent affecter les droits de choix et la vie privée des autres en sont un bon exemple.

6. Regroupement d'algorithmes pour une protection des données individuelle

Les systèmes de classification algorithmique soulèvent un défi pour les théories et les politiques de confidentialité existantes, car les politiques actuelles se concentrent principalement sur les informations personnelles et identifiables au niveau individuel, ce qui signifie que les demandes des individus de gérer les données les concernant prennent souvent fin une fois que les identifiants sont supprimés des données. Pourtant, le regroupement se fait davantage par le biais de formes algorithmiques de catégorisations impersonnelles du comportement et de la prédiction. Les jetons d'identité créés par le regroupement ne sont souvent pas réductibles aux individus du groupe, ni détenus par eux. Les décisions et politiques fondées sur le regroupement algorithmique affecteront néanmoins les intérêts des individus du groupe même si un tel groupement ne cible pas spécifiquement des individus identifiables. Profilage de groupes de consommateurs, solutions de notation et prédictives

les applications de police en sont plusieurs exemples.[52] Cela peut conduire à une discrimination de prix en fonction de l'affectation des consommateurs à un cluster spécifique, ou à une discrimination géographique qui affecte les personnes de certains quartiers, en particulier dans les cas, par exemple, de l'adoption de solutions de police prédictive qui s'accompagnent de biais d'algorithme non contrôlés.[53] La combinaison de différents types et sources de données pour l'analyse place les individus dans des groupes qui étaient auparavant non apparents ou inexistants.[54] Cela peut créer des groupes qui ne ressemblent pas nécessairement à des groupes historiquement protégés, auquel cas les lois de non-discrimination existantes peuvent être insuffisantes. Les victimes potentielles peuvent ne jamais être au courant du groupement et donc être incapables de déposer une plainte en vertu de la loi sur la non-discrimination.



2,3 Envisager les possibilités et les options

Pour relever ces nouveaux défis de la gouvernance technologique liés à l'IoB, une action multipartite est urgente. La section suivante présente un menu d'approches possibles, de la réglementation à la technologie, pour aider à atténuer ces risques afin de libérer pleinement le potentiel de l'IoB.

1. Construire un système de gouvernance solide et cohérent autour de l'internet des organes

Alors que l'internet des objets évolue de plus en plus pour être connecté aux corps humains, un système de gouvernance solide et cohérent est nécessaire pour faire face aux risques de l'expansion de l'IoB. Cela signifie que, par exemple, dans le contexte américain, une nouvelle stratégie de gouvernance devrait être formée à travers la division conventionnelle des domaines médicaux et non médicaux pour aborder la vaste dynamique des technologies et des données IoB. Certains experts suggèrent de combiner les pouvoirs de la FDA et de la FTC, ainsi que de la Consumer Product Safety Commission et du Consumer Financial Protection Bureau.[55] Les sénateurs Amy Klobuchar (D-MN) et Lisa Murkowski (R-AK) a introduit la loi sur la protection des données de santé personnelles en 2019 et a proposé la création d'un groupe de travail national chargé de protéger les données de santé.[56]

La gouvernance de l'IoB, comme dans le cas de l'IdO, repose non seulement sur les décideurs et les régulateurs, mais aussi sur des groupes professionnels, des associations industrielles, des groupes de patients, des utilisateurs et des citoyens, la société civile et d'autres formes de coopération multipartite, comme les technologies de l'IoB. sont pertinents pour la protection des droits humains fondamentaux dans un monde connecté.

2. Traiter les résultats des inférences et des analyses de données dans le domaine de la protection des données

Comme indiqué ci-dessus, les réglementations actuelles en matière de protection des données visent principalement à garantir que les données sont obtenues légalement et que leur traitement répond aux exigences des motifs légaux. Mais en général, les réglementations existantes ne parviennent pas à aborder les risques liés aux résultats du déploiement algorithmique dans tous les cas. Pour le dire simplement, ils concernent principalement les données d'entrée, plutôt que les nouvelles données générées par l'algorithme. L'IA et la réglementation des données devraient aborder les risques de confidentialité et de discrimination dans les inférences de données et l'analyse des algorithmes. Les experts en protection des données ont démontré que les progrès de l'analyse des mégadonnées exigent de nouvelles protections pour la confidentialité des groupes, répondant aux intérêts de confidentialité des groupes ad hoc formés par classification algorithmique.[57]

Différents du concept conventionnel de groupe, les groupes générés par algorithme sont caractérisés par une appartenance hautement dynamique au lieu d'une appartenance stable, et les individus regroupés dans un groupe peuvent même ne pas être conscients de leur appartenance. Il reste donc une tâche urgente de s'attaquer aux droits collectifs sur les données des groupes générés par des algorithmes, qui ne sont pas équivalents à la vie privée individuelle ni ne sont englobés par elle.[58]

Sandra Wachter et Brent Mittelstadt préconisent «un droit à des inférences raisonnables» pour combler le déficit de responsabilité posé par les «inférences à haut risque» et le risque de «discrimination par association».[59] Wachter souligne que pour lutter efficacement contre les risques d'inférence, une loi solide sur la protection des données devrait être complétée par des lois sectorielles agiles, en particulier dans les domaines à haut risque tels que la finance, l'emploi et la justice pénale. Cela nécessite un réexamen approfondi des lois sectorielles pour s'assurer qu'elles sont mises à jour pour faire face au risque de prise de décision algorithmique, car la plupart des lois anti-discrimination se concentrent sur la prévention de la discrimination dans les décisions humaines, mais ne parviennent pas à traiter l'opacité et l'imprévisibilité des algorithmes.[60]

3. Constituer un répertoire de technologies améliorant la protection de la vie privée et élaborer un cadre de prise de décisions

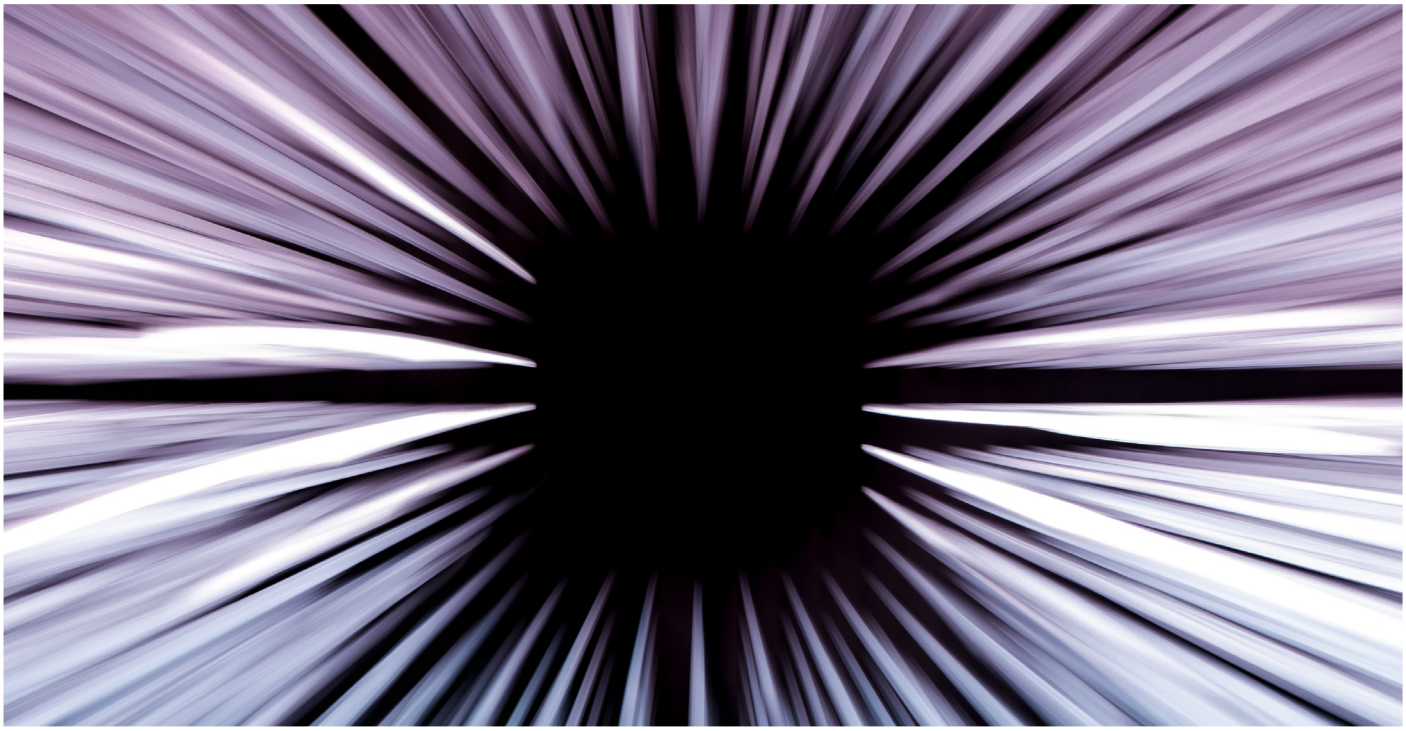
Un large éventail de solutions ou de méthodes technologiques a émergé pour atteindre des fonctionnalités spécifiques de protection de la vie privée ou des données, qui incluent le cryptage, la gestion des métadonnées et des droits numériques, la programmation d'applications, la gouvernance du développement de système, la gestion des identités, etc. Outre les méthodes bien connues de désidentification et de pseudonymisation , les données synthétiques constituent une autre approche de la dépersonnalisation des données. Les données synthétiques sont de «fausses» données qui ont les mêmes propriétés statistiques que les données réelles et peuvent être utilisées comme proxy pour des données réelles dans l'IA et l'apprentissage automatique, les tests de logiciels et à d'autres fins.[61] Alors que la désidentification, la pseudonymisation et les données synthétiques se concentrent sur la transformation des données, d'autres technologies abordent la protection des données par le contrôle des données. Récemment, un groupe des épidémiologistes et des data scientists au Royaume-Uni ont mené une étude sur les décès liés au COVID-19 parmi divers groupes de personnes et, d'extraction des dossiers médicaux sensibles de 17 millions de personnes à partir de bases de données, développé un logiciel pour exécuter l'analyse directement sur les données.[62] Cette approche de partage et d'analyse des données sensibles permet de contrôler les données sans les déplacer ni les divulguer.[63]

Étant donné que la conformité à la vie privée doit être considérée comme un éventail de risques, le choix spécifique de la technologie de protection de la vie privée est souvent pris en compte avec d'autres facteurs tels que l'utilité des données et le coût opérationnel. Un cadre de prise de décision peut aider à optimiser la solution dans chaque cas pour protéger la confidentialité des données de l'individu.[64]

4. Accompagnement des personnes concernées et expérimentation de l'approche solidaire

Une utilisation responsable de la technologie doit respecter les droits de l'homme et l'éthique.[65] Afin de tirer pleinement parti des avantages sociaux de la technologie et des données IoB, les utilisateurs devraient être dotés des droits légaux d'une personne concernée et d'un système de soutien pour exécuter ces droits. Cela nécessite une définition plus claire de la propriété des données et un meilleur contrôle des propres données des utilisateurs. Les utilisateurs seront soutenus par la connaissance de la manière dont leurs données sont utilisées et la capacité d'accéder à leurs informations et de les corriger, y compris les moyens de traiter les inférences et les analyses injustes.

En réponse au tri social et à la stratification alimentés par l'analyse Big Data, certains experts préconiser une approche solidaire de la gouvernance des données de santé (une approche axée sur le bien de la société et de la communauté).[66] Cela déplace l'attention vers les avantages et responsabilités sociétaux partagés, ce qui motive les gens à partager des données pour le bien collectif et individuel. Les biobanques sont un bon exemple de partage de données biologiques. L'approche solidaire de la gouvernance des données traite les contributeurs de données comme des partenaires, ce qui implique une reconnaissance explicite des types de recherche pris en charge par la base de données et un accès facile pour les membres de la communauté aux résultats de la recherche. Les personnes concernées doivent également être informées des risques potentiels associés à la participation.[67]



Contributeurs

Auteur principal

Xiao Liu
Membre du corps professoral de l'Université McGill au Centre du Forum économique mondial pour la quatrième révolution industrielle; Comité directeur Wilson China Fellow

Comité d'organisation

Jeff Merritt
Responsable, IoT, robotique et villes intelligentes, Centre pour la quatrième révolution industrielle, Forum économique mondial

Karime Kuri Tiscareno
Chef de projet, IoT, robotique et villes intelligentes, Centre pour la quatrième révolution industrielle, Forum économique mondial

Communauté d'experts

Ce livre blanc a bénéficié de la contribution de nombreux experts et de diverses parties prenantes qui ont partagé des études de cas, des idées et des leçons apprises à travers une série d'entretiens et de conversations en 2020.

Ifeoma Ajunwa
Professeur associé de droit du travail et de l'emploi, L'Université de Cornell; Associé de la faculté, Berkman Klein Centre de la Harvard Law School

Glenn Cohen
Professeur James A. Attwood et Leslie Williams of Law, Harvard Law School; Directeur de Faculté, Petrie-Flom Centre for Health Law Policy, Biotechnology & Bioethics

Jim Dempsey
Directeur exécutif, Berkeley Center for Law & La technologie

K haled El Emam
Scientifique principal, Institut de recherche du CHEO; Professeur, pédiatrie, faculté de médecine, Université d'Ottawa; Président-directeur général, Privacy Analytics

Tad Funahashi
Kaiser Permanente / SCPMG, chef de l'innovation Officier, chirurgie orthopédique et médecine du sport

Jodi Halpern
Professeur de bioéthique et humanités médicales, Université de Californie, Berkeley

Jiang Li
Directeur général, VivaLNK, Connected Healthcare Solutions

Xuan Hong Lim
Gestionnaire principal, Smart Nation et numérique Groupe gouvernemental, gouvernement de Singapour

Alex Mihailidis
Vice-président associé - International Partenariats, Université de Toronto; Scientifique Directeur - AGE-WELL NCE

Piers Nash
Directeur général, Sympatic

Kim Old
Directeur commercial, EMOTIV

Olivier Oullier
Président, EMOTIV, USA

Margaret Foster Riley
Professeur de droit, Université de Virginie

Lee Tien
Avocat principal et président Adams pour les droits Internet, Electronic Frontier Foundation

Jennifer M. Urban
Professeur clinique de droit Directeur des initiatives politiques, Samuelson Law, Technology & Public Policy Clinic, Université de Californie, Berkeley

Sandra Wachter
Professeur associé et chercheur principal, Oxford Internet Institute, Université d'Oxford

Remerciements

Ce livre blanc a bénéficié des idées, des commentaires, des conversations et des contributions de collègues du Centre pour la quatrième révolution industrielle du Forum économique mondial. Remerciement spécial à:

Kimmy Bettinger
Spécialiste, IoT, Robotique et villes intelligentes, Centre du Forum économique mondial pour la quatrième révolution industrielle

Lynsey Chediak
Chef de projet, Médecine de précision, Centre du Forum économique mondial pour la quatrième révolution industrielle

Anne Joséphine Flanagan
Chef de projet, Politique des données, Centre du Forum économique mondial pour la quatrième révolution industrielle

Arthur Hermann
Kaiser Permanente, ancien membre du Forum économique mondial

Austin Hunter
Spécialiste, Politique des données, Centre du Forum économique mondial pour la quatrième révolution industrielle

Eddan Katz
Curateur de la plateforme: Intelligence artificielle, Centre du Forum économique mondial pour la quatrième révolution industrielle; Ancien membre du Forum économique mondial

Elissa Prichep
Chef de projet, Médecine de précision, Centre du Forum économique mondial pour la quatrième révolution industrielle

Geoff Wylde
Chef de projet, IoT, Robotique et villes intelligentes, Centre du Forum économique mondial pour la quatrième révolution industrielle

Notes de fin

1. Managing Epidemics with Consumer Wearables, Forum économique mondial: https://www.weforum.org/covid-actionplatform/projects/managing-epidemics-with-consu (lien au 1/7/20).
2. Andrea M. Matwyshyn, L'Internet des corps, William & Mary Law Review, Vol. 61, n ° 1, 2019. Ibid.
3.
4. Ibid.
5. Par exemple, aux États-Unis, la FDA considère un produit comme un appareil, et soumis à la réglementation de la FDA, s'il répond à la définition d'un dispositif médical selon la section 201 (h) de la Food, Drug, and Cosmetic Act. Les dispositifs médicaux sont: a) reconnus dans le Formulaire national officiel, ou dans la Pharmacopée des États-Unis, ou dans tout supplément à ceux-ci; b) destiné à être utilisé dans le diagnostic d'une maladie ou d'autres conditions, ou dans la guérison, l'atténuation, le traitement ou la prévention d'une maladie,
chez l'homme ou d'autres animaux; c) ou destinés à affecter la structure ou toute fonction du corps de l'homme ou d'autres animaux. Voir https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device#steps .
6. Des milliers de Suédois insèrent des micropuces sous leur peau, NPR, 2018: https: //www.npr. org / 2018/10/22/658808705 / des milliers-de-suède-insèrent-des-puces-sous-leur-peau (lien au 1/7/20).
7. J'ai une puce implantée dans un garage de biohacking, Freethink, 2020: https://www.freethink.com/videos/biohacking (lien au 1/7/20).
8. Valuates Report, la taille du marché des technologies portables devrait atteindre 57653 millions USD d'ici la fin de 2022, avec un TCAC de 16,2, PR Newswire, février 2020: https://www.prnewswire.com/news-releases/wearable-technology-marketsize-is-expected-to-reach-usd-57-653-millions-by-the-end-of-2022--w -cagr-of-16-2 - évalue-rapports-301001809. html (lien au 1/7/20).
9. Voir le rapport d'étude de marché d'IDTechEX, Electronic Skin Patches 2019–2029: https://www.idtechex.com/en/researchreport/electronic-skin-patches-2019-2029/67 (lien au 1/7/20).
dix. Ryan Kraudel, Une enquête nationale sur les appareils portables révèle l'accélération de la convergence des appareils portables grand public et de la santé personnelle et des dispositifs médicaux, Valencell, novembre 2019: https://valencell.com/press/2018/11/national-wearables-surveyreveals-accelerating-convergence-of-consumer-wearables-and-person (lien au 1/7/20).
11. Un bon exemple de cela: Alex Mihailidis et son équipe de Intelligent Assistive Technology and Systems Lab à Toronto ont développé un environnement intelligent de soutien pour aider les patients et les utilisateurs plus âgés avec des fonctions de surveillance de la santé et de détection des chutes.
12. VivaLNK propose une solution de surveillance des patients à distance à déploiement rapide avec Alibaba, PR Newswire, mars 2020: https://www.prnewswire.com/news-releases/vivalnk-offers-rapid-deployment-remote-patient-monitoring-solution-withalibaba-301013155.html (lien au 1/7/20).
13. Agam Shah, Kaiser Permanente Bets on Smartwatches to Lower Costs, Wall Street Journal, janvier 2020: https: // www. wsj.com/articles/kaiser-permanente-bets-on-smartwatches-to-lower-costs-11578565801 (lien au 1/7/20).
14. Cinq ans et 500 études de recherche Fitbit, Fitabase, décembre 2017: https://www.fitabase.com/blog/post/five-years500-fitbit-research-studies/ (lien au 1/7/20).
15. IBM aide les organisations à surveiller la sécurité de leurs travailleurs avec Watson IoT, IBM, février 2019: https://newsroom.ibm. com / 2019-02-13-IBM-Aide-les-organisations-Surveiller-la-sécurité-de-leurs-travailleurs-avec-Watson-IoT (lien au 1/7/20).
16. Julie Weed, technologie portable qui dit aux camionneurs somnolents qu'il est temps de s'arrêter, New York Times, février 2020: https: // www.nytimes.com/2020/02/06/business/drowsy-driving-truckers.html (lien à partir du 07/02/20).
17. Maarten Falter et. al, Précision des mesures Apple Watch pour la fréquence cardiaque et les dépenses énergétiques chez les patients atteints de maladie cardiovasculaire: étude transversale, JMIR Mhealth Uhealth 2019; Vol. 7, n ° 3, mars 2019, e11889: http: // doi.org/10.2196/11889 (lien au 1/7/20).
18. Emily J. Shiffer, Quelle est la précision du moniteur de fréquence cardiaque d'Apple Watch pour la détection d'Afib? Il ne peut pas remplacer les appareils de qualité médicale, Insider, mai 2020: https://www.insider.com/how-accurate-is-apple-watch-heart-rate (lien au 1/7/20).
19. Zoë LaRock, l'année dernière, les soins de santé ont connu plus de violations de la cybersécurité que tout autre secteur - et cela va probablement s'intensifier, Business Insider, avril 2019: https://www.businessinsider.com/why-healthcare-data-breach-epidemic-willintensify-2019-4 (lien au 1/7/20).
20. Alfred Ng, Les montres intelligentes de ces enfants ont des problèmes de sécurité aussi simples que 1-2-3, CNet, décembre 2019: https: // www. cnet.com/news/these-kids-smartwatches-have-security-problems-as-simple-as-1-2-3/ (lien au 1/7/20).
21. Liz Sly, des soldats américains révèlent des informations sensibles et dangereuses par Jogging, Washington Post, janvier 2019: https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-ussoldiers-are-and-what-they-are-faire / 2018/01/28 / 86915662-0441-11e8-aa61-f3391373867e_story.html (lien au 1/7/20).
22. Jane C. Hu, Alors à propos de ces données de thermomètre qui indiquent que les fièvres sont en déclin, Ardoise, avril 2020: https://slate.com/ technology / 2020/04 / kinsa-smart-thermometer-data-fevers-covid19.html (lien au 1/7/20).

23. Florence Hudson et Chris Clark, Wearables and Medical Interoperability: The Evolving Frontier, Computer, vol. 51, No. 9, 2018, pp. 86–90, doi: 10.1109 / MC.2018.3620987 (lien au 1/7/20).

24. Marshall Allen, les assureurs-maladie aspirent des détails sur vous - et cela pourrait augmenter vos tarifs, ProPublica, juillet 2018: https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about- vous-et-pourriez-augmenter-vos-taux (lien au 1/7/20); Mohana Ravindranath, Comment vos informations de santé sont vendues et transformées en scores de risque, Politico, février 2019: https://www.politico.com/story/2019/02/03/health (lien au 1/7/20).

25. Ifeoma Ajunwa souligne que les lois existantes sur la protection de la vie privée contiennent toujours des exceptions centrées sur l'employeur, et la jurisprudence a montré que peu de protections existent lorsqu'un employé consent à la collecte d'informations. Voir Ifeoma Ajunwa, Algorithms at Work: Productivity Monitoring Platforms and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labour Law, St.Louis Law Journal, 21 (2019). Il existe déjà de nombreuses poursuites concernant un comportement suspect de l'employeur en ce qui concerne les plans de bien-être des employés et les applications de productivité au travail. Voir Ajunwa et al, Limitless Worker Surveillance, California Law Review, vol. 105, n ° 3, 2017, pp. 735–776; et Ajunwa, Algorithmes au travail.

26. Miranda Bogen, All the Ways Hiring Algorithms Can Introduce Bias, Harvard Business Review, 6 mai 2019: https: // hbr. org / 2019/05 / tous-les-algorithmes-d'embauche-peuvent-introduire-un-biais (lien à partir du 6/7/20).

27. Voir Katherine Kellogg et al., Algorithm at Work: The New Contested Terrain of Control, Academy of Management: https://doi.org/10.5465/annals.2018.0174 (lien au 1/7/20), pour plus de détails sur comment les algorithmes exacerbent le contrôle sur le lieu de travail, et pour des exemples de l'action des employés et des militants pour lutter contre ces contrôles.

28. Lena Solow, Le fléau des programmes de mieux-être des travailleurs, Nouvelle République, septembre 2019: https://newrepublic.com/ article / 154890 / scourge-worker-wellness-programmes (lien au 1/7/20).

29. Jessica Bruder, Ces travailleurs ont une nouvelle demande: Arrêtez de nous regarder, The Nation, mai 2015: https: //www.thenation. com / article / archive / ces-travailleurs-ont-une-nouvelle-demande-arrêter-de nous regarder / (lien au 1/7/20); Esther Kaplan, L'espion qui m'a viré, Harpers, mars 2015: https://harpers.org/archive/201 (lien au 1/7/20).

30. Voir Sean McDonald, Ebola: A Big Data Disaster, CIS Papers, mars 2016: https://cis-india.org/papers/ebola-a-big-datadisaster (lien au 1/7/20). Les politiques publiques fondées sur l'analyse des données sont particulièrement risquées dans les pays moins développés et parmi les populations défavorisées où les informations et les infrastructures réglementaires sont insuffisantes. Linnet Taylor, la sécurité en chiffres? Group Privacy and Big Data Analytics in the Developing World, in Linnet Taylor et al., Éditeurs, Group Privacy - New Challenges of Data Technologies, Springer, 2017: pp. 13–36.

31. Directives concernant les méthodes de désidentification des informations de santé protégées conformément à la règle de confidentialité de la loi HIPAA (Health Insurance Portability and Accountability Act): https://www.hhs.gov/hipaa/for-professionals/privacy/ special-topics / de-identification / index.html (lien au 1/7/20).

32. Loi sur la Commission fédérale du commerce: https://www.ftc.gov/enforcement/statutes/federation-trade-commission-act (lien à partir du 07/02/20).

33. Florent Thouvenin et al., Big Data dans le secteur de l'assurance: marge de manœuvre et limites pour individualiser les contrats d'assurance: https://www.jipitec.eu/issues/jipitec-10-2-2019/4916 (lien au 1/7/20).

34. Sharona Hoffman, Big Data's New Discrimination Threats: Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease, in I.Glenn Cohen et al., Éditeurs, Big Data, Health Law and Bioethics, Cambridge University Press , 2018, pp. 85–97.

35. Pour un aperçu des lois sur la confidentialité des États, voir Andy Green, Guide complet des lois sur la confidentialité aux États-Unis, Varonis, mars 2020: https://www.varonis.com/blog/us-privacy-laws/ (lien au 1/7/20).

36. Kathryn C.Montgomery, Jeff Chester et al., Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection, Center for Digital Democracy, août 2017: https://www.democraticmedia.org/CDD-WearableDevices-Big-Data-Report (lien au 1/7/20).

37. Charte des droits fondamentaux de l'Union européenne 2012 / C 326/02: https://eur-lex.europa.eu/legal-content/EN/TXT/ HTML /? uri = CELEX: 12012P / TXT & from = EN (lien au 1/7/20).

38. Directive 2002/58 / CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive sur la vie privée et les communications électroniques): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?u (lien au 1/7/20).

39. Art. 4 (15) du RGPD. Art.22

40. du RGPD.

41. Sandra Wachter, Profil d'affinité et discrimination par l'Association dans la publicité comportementale en ligne, Berkeley Technology Law Journal, Vol. 35, n ° 2, 2020.

42. Oliver Jérusalmy et Paul Fox, Insurance and Discrimination - Guaranteeing Full and Equal Access to Insurance, Finance Watch, 28 février 2019: https://www.fina (lien au 1/7/20).

43. W. Nicholson Price II et I. Glenn Cohen, La vie privée à l'ère des mégadonnées médicales, Nature Medicine, Vol. 25, 2019, p. 37–43.

44. Kashmir Hill, Comment Target a découvert qu'une adolescente était enceinte avant que son père ne le fasse, Forbes, février 2012: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-fatherdid/#578f4eeb6668 (lien à partir du 07/02/20).

45. Margaret Foster Riley, Big Data, HIPAA, and the Common Rule: Time for Big Change ?, in I. Glenn Cohen et al., Éditeurs, Big Data, Health Law, and Bioethics, Cambridge University Press, 2018, p. 251– 263.

46. Paul Ohm, Promesses brisées de confidentialité: répondre à l'échec surprenant de l'anonymisation, UCLA Law Review, Vol. 57, 2010, p. 1701.

47. Mark Rothstein, La désidentification est-elle suffisante pour protéger la confidentialité en matière de santé dans la recherche? L'American Journal of Bioethics, Vol. 10, n ° 9, septembre 2010, p. 3–11, doi: 10.1080 / 15265161.2010.494215 (lien à partir du 07/02/20).

48. Sandra Wachter et Brent Mittelstadt, A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI, Columbia Business Law Review, 2019 (2).

49. Wachter, profilage d'affinité et discrimination par association dans la publicité comportementale en ligne.

50. Alessandro Mantelero, L'avenir de la protection des données des consommateurs dans l'UE: repenser le paradigme de «l'avis et du consentement» dans la nouvelle ère de l'analyse prédictive, Computer Law & Security Review, Vol. 30, n ° 6, 2014, pp. 643–660.

51. Barbara J. Evans, Big Data and Individual Autonomy in a Crowd, dans I. Glenn Cohen et al., Éditeurs, Big Data, Health Law, and Bioethics, Cambridge University Press, 2018, p. 19-29.

52. Alessandro Mantelero, Données personnelles à des fins décisionnelles à l'ère de l'analytique: d'une dimension individuelle à une dimension collective de la protection des données, du droit informatique et de la sécurité, Vol. 32, n ° 2, 2016, pp. 238-255.

53. Ibid.

54. Brent Mittelstadt, De la vie privée individuelle au groupe dans l'analyse, la philosophie et la technologie du Big Data, 30, 2017, 4, pp. 475–494.

55. Matwyshyn, L'Internet des corps.

56. Loi sur la protection des données personnelles sur la santé: https://www.congress.gov/bill/116th-congress/senate-bill/1842/text/is (lien au 1/7/20).

57. Linnet Taylor, Luciano Floridi et al., Éditeurs, Group Privacy: New Challenges of Data Technologies, Springer, 2017; Mantelero, Données personnelles à des fins décisionnelles à l'ère de l'analytique: d'une dimension individuelle à une dimension collective de la protection des données.

58. Ibid.

59. Voir Wachter et Mittelstadt, A Right to Reasonable Inferences: Repenser la loi sur la protection des données à l'ère du Big Data et de l'IA; et Wachter, Profilage d'affinité et discrimination par association dans la publicité comportementale en ligne.

60. Entretien avec Sandra Wachter par Xiao Liu le 22 mai 2020. Voir Qu'est-ce que les données synthétiques ?, Replica Analytics: https://www.replica-analytics.com/synthesis-tutorials

61. (lien à partir du 07/02/20).

62. La pandémie a engendré une nouvelle façon d'étudier les dossiers médicaux, The Economist, mai 2020: https: //www.economist. com / science-et-technologie / 2020/05/14 / la-pandémie-a-engendré-une-nouvelle-façon-d'étudier-les-dossiers-médicaux (lien à partir du 07/02/20).

63. La technologie cloud de Sympatic, appelée «VirtualVault», est un autre exemple de cette approche pour permettre à «l'ordinateur» d'accéder aux données. Voir https://www.sympa (lien au 1/7/20).

64. Le chercheur canadien Khaled El Emam a développé un cadre basé sur la recherche existante et les pratiques commerciales qui prennent en considération différents facteurs, de la protection de la vie privée, de l'utilité des données et des coûts opérationnels à la confiance des consommateurs. Les responsables du traitement peuvent attribuer un poids à ces facteurs en fonction des exigences réglementaires et de leurs propres besoins pratiques et trouver la meilleure combinaison de solutions. Voir Quand synthétiser: https://www.replica-analytics.com/sy (lien au 1/7/20).

65. Pour une approche éthique de la technologie responsable, voir Utilisation responsable de la technologie, livre blanc du Forum économique mondial, août 2019: http://www3.weforum.org/docs/WEF_Responsible_Use_of_Technology.pdf (lien au 1/7/20)

66. Barbara Prainsack et Ine Van Hoyweghen, Shifting Solidarities: Personalization in Insurance and Medicine, in Ine Van Hoyweghen, Valeria Pulignano et Gert Meyers, éditeurs, Shifting Solidarities: Trends and Developments in European Societies, Palgrave Macmillan, 2020 (à paraître). Aperçu disponible sur: https://www.researchgate.net/ publication / 338254212_Shifting_Solidarities_Personalisation_in_insurance_and_medicine (lien au 1/7/20).

67. Ibid.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Le Forum économique mondial, engagé à améliorer l'état du monde, est l'Organisation internationale pour Coopération public-privé.

Le Forum engage les principaux acteurs politiques et commerciaux et d'autres leaders de la société pour façonner les programmes mondiaux, régionaux et industriels.

Forum économique mondial
91–93 route de la Capite CH-1223
Cologny / Genève
Suisse

Tél .: +41 (0) 22869 1212 Fax:
+41 (0) 22786 2744
contact@weforum.org
www.weforum.org