4.7 FIABILITÉ DES TECHNOLOGIES ET DES DONNÉES

L'accès à l'information est un droit humain fondamental qui a joué un rôle majeur pour le développement durable dans des domaines tels que la santé, l'environnement, la réduction de la pauvreté et la lutte contre la corruption. Compte tenu des énormes quantités de données et d'informations transmises et/ou stockées quotidiennement, les entreprises doivent prendre des engagements durables concernant l'ODD n°16. Plus les données sont fiables, plus elles permettent de prendre des décisions avisées, lesquelles sont cruciales pour contribuer à un avenir durable. Les entreprises doivent donc veiller à ce que la collecte, le stockage, l'extraction et la diffusion des données soient effectués de manière responsable et sécurisée. La sécurité de l'information est au cœur de cette problématique.

Les entreprises sont confrontées à des cybermenaces qui évoluent en permanence et qui entraînent des coûts supplémentaires liés aux aspects juridiques, réglementaires et techniques, à la perte de l'image de marque, à la perte de clientèle et à la baisse de la productivité des employés.

Les répercussions d'une cyberattaque peuvent être très préjudiciables. Les entreprises encourent des amendes et doivent gérer de coûteuses procédures de notification de violation. Qui plus est, ces attaques entraînent souvent des interruptions d'activité et une publicité négative. Renforcer la sécurité des informations est une étape nécessaire et logique pour suivre le rythme effréné de la dématérialisation engagée par les entreprises au cours de la dernière décennie.

Cette progression rapide de la numérisation mondiale a amélioré l'efficacité et l'efficience de nos vies, tant personnelles que professionnelles, mais nous devons également être davantage conscients et mieux comprendre les dangers, involontaires ou intentionnels, qu'elle engendre. Comment pouvons-nous atténuer les risques technologiques et prévoir les éventuelles menaces ? Il faut trouver un juste équilibre pour ne pas freiner l'innovation et mettre en place une surveillance suffisante. Un certain degré de collaboration entre les secteurs public et privé peut aider à atteindre les objectifs d'une technologie fiable. Certains craignent que quelques entreprises n'exercent une influence et un contrôle excessifs sur la technologie et la sphère de l'information. Les conséquences réelles et éventuelles de cette situation soulèvent de vastes questions sur le plan ESG. L'impartialité de l'intelligence artificielle (IA) et des algorithmes peut-elle être garantie ? Qui décide de ce qui est juste et de ce qui est interdit ? En fin de compte, quand devrions-nous NE PAS faire confiance à la technologie ou aux données et donc à l'organisme qui les a produites ?

20. De plus amples informations sont disponibles sur le site Internet de Cisco

4.7 FIABILITÉ DES TECHNOLOGIES ET DES DONNÉES

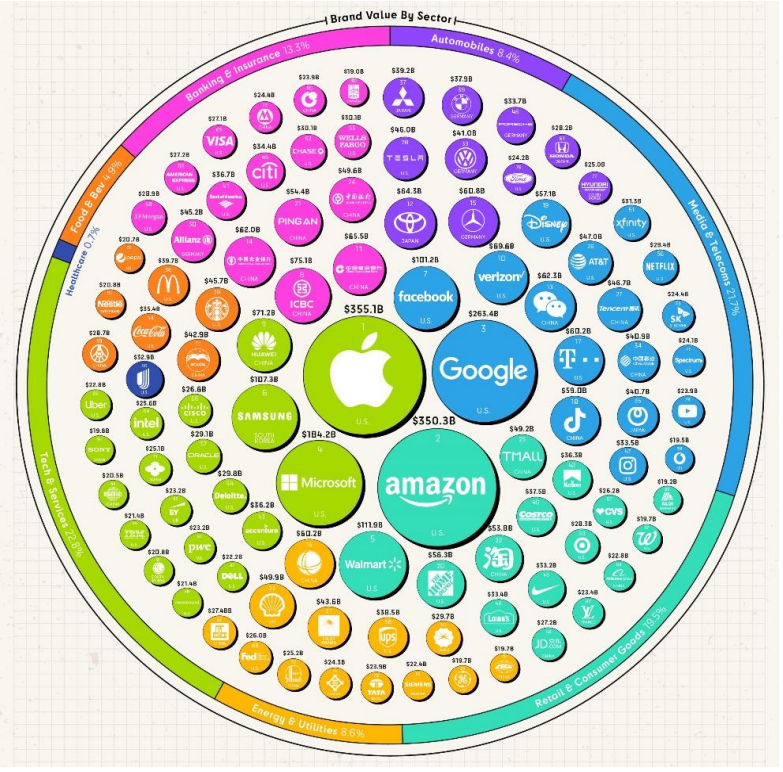
Les entreprises adoptent de plus en plus l'IA et l'apprentissage automatique dans leur processus décisionnel, ce qui implique un accès aux données et à leur analyse ainsi qu'une meilleure compréhension de ces dernières. Cela peut améliorer la qualité de la prise de décision, mais de nouvelles cyberstratégies devront être élaborées, qui mettront davantage l'accent sur la protection de l'identité numérique des entreprises et des particuliers et sur la prévention de la fraude. Ce sont des domaines qui peuvent être renforcés et favorisés par l'adoption croissante de l'IA et de l'apprentissage automatique.

Une infrastructure résiliente est indispensable pour garantir la fiabilité des données, car la sécurité ne peut être sacrifiée au profit de l'efficacité et de l'efficience. Les entreprises doivent également explorer des alternatives fiables aux modèles économiques actuels, en accordant la priorité aux facteurs humains et sociaux, tout en mettant en œuvre des indicateurs de performance technique pertinents. Les réseaux « zero trust "[20] (où l'accès au réseau fait l'objet d'une authentification permanente pour garantir la sécurité des données) sont appelés à devenir la norme pour se conformer à une réglementation plus stricte. La sécurité des points d'accès peut englober les appareils mobiles et des solutions biométriques pour compenser l'augmentation des attaques liées au travail à distance. La vigilance doit s'étendre à la cyberchaîne d'approvisionnement, comme le Cloud et les plateformes SaaS.

On assiste aujourd'hui à une accélération des technologies numériques et à une explosion du volume de données, ce qui permet une croissance socio-économique inédite. Cependant, malgré toutes les opportunités que cela offre, nous ne devons pas négliger les problèmes ESG que cela engendre sur les plans économique, social et éthique, et qui, tous, augmentent les risques auxquels est exposée une entreprise. En 2022, plusieurs grandes entreprises technologiques bien connues ont fait l'objet de propositions d'actionnaires lors de leurs assemblées générales, et nous pensons que ce thème va prendre de l'ampleur. Cela obligera les entreprises à se montrer plus responsables et à mieux gérer les questions connexes, ce qui devrait amener HSBC AM à affiner son approche et ses attentes.

Il n'est pas surprenant de constater que bon nombre des marques les plus appréciées au monde (voir page suivante) sont fortement liées ou doivent une grande partie de leur succès aux progrès de la technologie et à la capacité du monde à accéder à l'information.

20. De plus amples informations sont disponibles sur le site Internet de Cisco



Source : visualcapitalist.com

Selon Lobbyfacts.EU, le nouvel entrant le plus important dans le top 50 des lobbies d'entreprise les plus dépensiers en 2022 est l'industrie technologique. Lobbyfacts.EU a également révélé que les entreprises technologiques occupaient une place prépondérante dans le top 10 des entreprises les plus dépensières en 2022[21].

Notre position

Dans la mesure où le fait de disposer de technologies et de données fiables constitue le fondement des environnements numériques, y compris le métavers, les entreprises technologiques investissent massivement dans leur développement et dans la promotion de leur adoption dans le but d'affirmer leur domination et éventuellement de créer des positions de leader sur le marché du matériel, des logiciels, des médias sociaux, des cryptoactifs et des données.

Nous devons reconnaître et accepter que la technologie et les données ont et continueront d'avoir un impact positif sur la société à l'échelle mondiale. Comme on a pu le constater au cours des 36 derniers mois, d'abord en raison de la pandémie de COVID-19, la médecine, la science et l'éducation ont toutes bénéficié des progrès, de l'intégration et de l'utilisation de ces technologies. Pour autant, les risques liés à la collecte abusive de données, à la surveillance omniprésente et à une modération insuffisante sont plus importants que jamais. Une fois qu'elles sont collectées, les utilisateurs ne peuvent pas faire grand-chose pour atténuer les préjudices causés par les fuites de données ou leur monétisation par des tiers. Les appareils collecteront également d'énormes quantités de données sur nos habitations et nos espaces privés, ce qui permettra aux gouvernements, aux entreprises et aux forces de l'ordre d'accéder à nos vies sans notre consentement, et donc de multiplier les intrusions dans la vie privée.

21. LobbyFacts offre aux journalistes, activistes et chercheurs la possibilité de rechercher, trier, filtrer et analyser les données du registre de transparence officiel de l'UE, afin de suivre les activités des lobbyistes et leur influence au niveau de l'UE au fil du temps. De plus amples informations sont disponibles sur leur site Internet.

4. Nos principaux thèmes de dialogue (suite)

Avec l'introduction ou la révision de la législation relative au numérique au Royaume-Uni, aux États-Unis et en Europe, ainsi que la reconnaissance officielle par les Nations unies que l'espace numérique doit également respecter les droits de l'homme, les entreprises les plus proactives vont devoir commencer à formuler et à mettre en œuvre des politiques spécifiques pour faire face à ce défi. Notre engagement sur ce thème nous a amenés à jouer un rôle de premier plan au sein de la World Benchmarking Association, notamment à propos de l'inclusion numérique et de l'intelligence artificielle éthique (« IA »).

Avoir accès à Internet, au métavers et à des applications nécessite une technologie fiable ; la fourniture de ces équipements peut favoriser l'inclusion, mais le fabricant/fournisseur de ce type d'appareils a-t-il un devoir légal de vigilance vis-à-vis de l'utilisateur direct et même des tierces parties qui interagissent avec l'utilisateur direct ? Et si oui, dans quelle mesure ?

Nos initiatives

Dans le cadre de nos interventions auprès des entreprises, nous rechercherons et évaluerons les mesures positives qu'elles ont prises en matière de technologies et de données fiables et qui contribuent à l'adoption de pratiques environnementales et sociales responsables. Nos échanges tendront à encourager les entreprises à limiter les coûts potentiels en s'attaquant aux risques et en améliorant leur approche globale de ce thème.

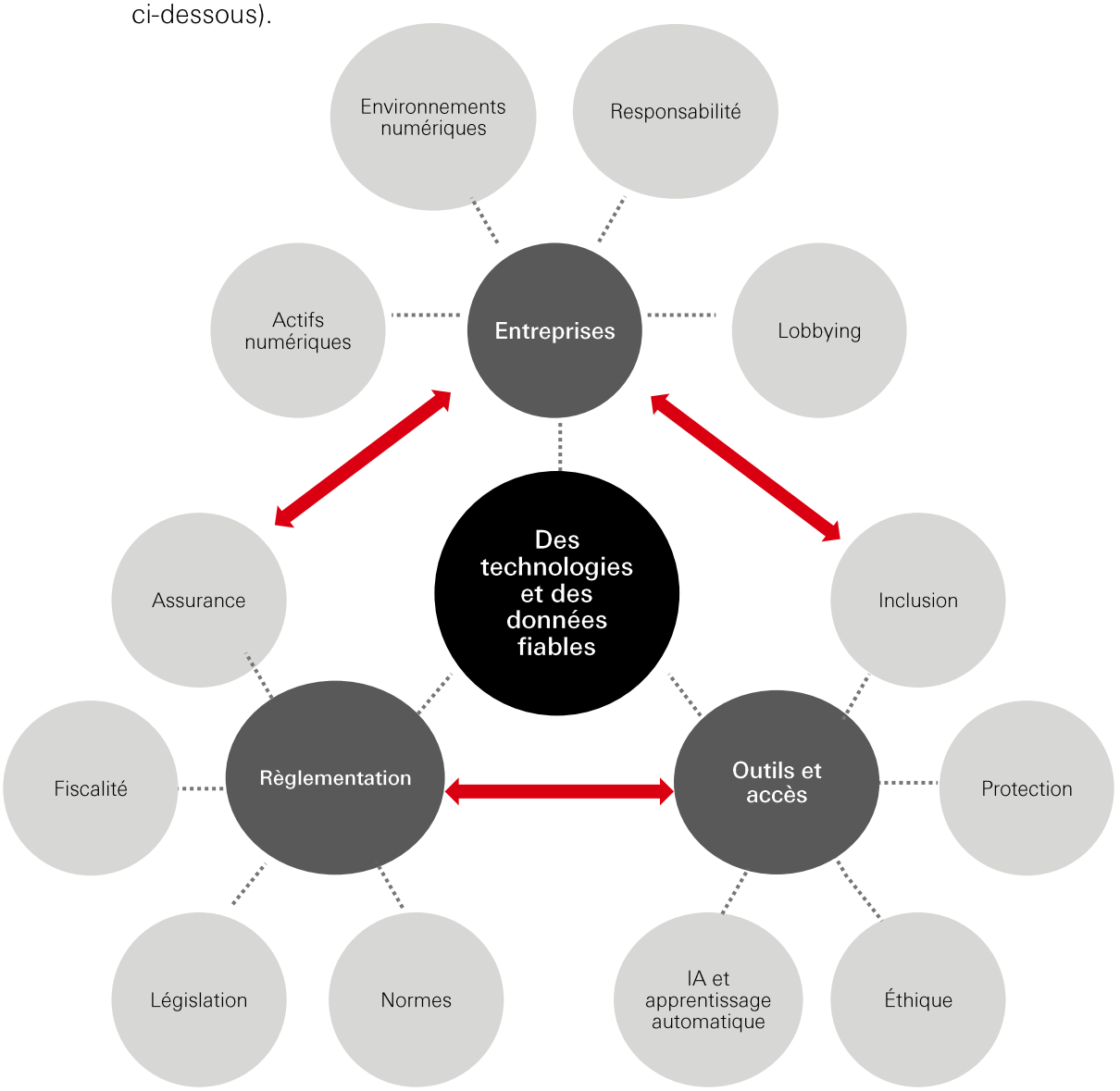
Nous examinerons si des stratégies efficaces de protection, de sécurité et de prévention ont été intégrées dans les politiques de protection de l'information. Cette question fait partie des principales responsabilités du conseil d'administration en matière de surveillance des risques. À l'échelle mondiale, les conseils d'administration devront rendre des comptes pour tout impact négatif dû à leur incapacité présumée à mettre en place des instances de gouvernance appropriées pour se protéger contre les cyberrisques.

Le fait de savoir si la responsabilité des entreprises en matière de respect des droits de l'homme s'étend aux questions liées à l'environnement numérique et les aborde est une question cruciale. Est-ce que l'entreprise prend des mesures constructives et proactives pour défendre, protéger et respecter les droits de l'homme pour le bien-être général de ses utilisateurs dans un environnement numérique ? Les entreprises sont confrontées à un défi : elles doivent à la fois s'efforcer de ne pas faire obstacle au respect des droits de l'homme, tout en veillant à garantir une protection contre tout préjudice implicite ou réel. L'existence d'un comité totalement indépendant et dirigé par des experts, chargé de veiller au respect et à la défense des droits de l'homme dans l'environnement numérique, serait idéale. Dans la mesure du possible, la question de la transparence et de la responsabilité en matière de contenu doit être prise en compte. Il convient de sensibiliser les employés et les utilisateurs à la collecte, au stockage, au traitement et à la diffusion des données, tout en garantissant la protection des données et du droit à la vie privée des utilisateurs.

Notre approche

Nous cherchons à identifier et à encourager un meilleur alignement des politiques et des pratiques des entreprises sur les normes et les obligations énoncées par les principes directeurs des Nations unies. Les entreprises doivent s'efforcer de faire preuve d'une plus grande vigilance à l'égard de leurs modèles d'entreprise ou de leurs activités qui risquent de porter atteinte aux droits de l'homme.

Lorsque nous nous impliquons auprès d'une entreprise, nous utilisons Ranking Digital Rights[22] et le Digital Inclusion Benchmark[23] de la World Benchmarking Alliance (WBA) comme références lors de notre évaluation. Les investisseurs sont de plus en plus nombreux à s'intéresser aux formidables opportunités qu'offre l'univers du numérique. Nous pouvons donc nous attendre à une offre plus large de produits associés au numérique, alimentés par l'augmentation des dépenses d'investissement des entreprises. Bénéfices et protection doivent être les deux faces d'une même pièce (voir ci-dessous).



22. Ranking Digital Rights vise à promouvoir la responsabilité des entreprises en matière de droits de l'homme à l'ère numérique. De plus amples informations sont disponibles sur leur site Internet.
23. Le Digital Inclusion Benchmark suit la manière dont les entreprises contribuent à faire progresser une économie et une société numériques plus inclusives. De plus amples informations sont disponibles sur leur site Internet.

Informations importantes

Cette politique est produite et diffusée par HSBC Asset Management et est destinée aux investisseurs non-professionnels et professionnels au sens de la directive européenne MIF. L'ensemble des informations contenu dans ce document peut être amené à changer sans avertissement préalable. Toute reproduction ou utilisation (même partielle), sans autorisation, de ce document engagera la responsabilité de l'utilisateur et sera susceptible d'entraîner des poursuites. Ce document ne revêt aucun caractère contractuel et ne constitue en aucun cas ni une sollicitation d'achat ou de vente, ni une recommandation d'achat ou de vente de valeurs mobilières dans toute juridiction dans laquelle une telle offre n'est pas autorisée par la loi.
Les commentaires et analyses reflètent l'opinion de HSBC Asset Management sur les marchés et leur évolution, en fonction des informations connues à ce jour. Ils ne sauraient constituer un engagement de HSBC Asset Management.
En cas de besoin, les investisseurs peuvent se référer à la charte de traitement des réclamations disponible dans le bandeau de notre site internet et sur le lien suivant :
https://www.assetmanagement.hsbc.fr/-/media/files/attachments/france/common/traitement-reclamation-amfr-vf.pdf
Il est à noter que la commercialisation du produit peut cesser à tout moment sur décision de la société de gestion
En conséquence, HSBC Asset Management ne saurait être tenue responsable d'une décision d'investissement ou de désinvestissement prise sur la base de ces commentaires et/ou analyses.
Toutes les données sont issues de HSBC Asset Management sauf avis contraire. Les informations fournies par des tiers proviennent de sources que nous pensons fiables mais nous ne pouvons en garantir l'exactitude. Le caiptal n'est pas garanti.
HSBC Asset Management est la marque commerciale de l'activité de gestion d'actifs du Groupe HSBC, qui comprend les activités d'investissement fournies par nos entités locales réglementées.
HSBC Global Asset Management (France) - 421 345 489 RCS Nanterre. S.A au capital de 8.050.320 euros.
Société de Gestion de Portefeuille agréée par l'Autorité des Marchés Financiers (n° GP99026)
Adresse postale : 38 avenue Kléber 75116 PARIS
Siège social : Immeuble Coeur Défense | 110, esplanade du Général de Gaulle - La Défense 4 - 92400 Courbevoie - France
www.assetmanagement.hsbc.fr
Document non contractuel, mis à jour en juin 2023

AMFR_2023_ESG_ESG_0900. Expiration: 06/2024