ARCSI
Association des Réservistes du Chiffre
et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité » n°62
Lundi 23 octobre 2023

Cybersécurité et intelligence artificielle
Perspective transdisciplinaire et sociétale

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 1 Cybersécurité et E-santé

SOMMAIRE

Introduction

Le "Lundi de la Cybersécurité" n°62, intitulé "Cybersécurité et Intelligence Artificielle - Perspective transdisciplinaire et sociétale," a marqué un moment crucial pour l'exploration des défis et opportunités qui découlent de l'intersection de la cybersécurité et de l'intelligence artificielle. Cet événement en ligne, orchestré par un comité d'experts de renom comprenant le Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks, a rassemblé une assemblée de professionnels et de chercheurs œuvrant dans ces domaines interconnectés.

Objectif de la Conférence :

Le but primordial de cette conférence était de dévoiler les arcanes de l'avenir numérique. En se penchant sur l'impact grandissant de l'intelligence artificielle sur la cybersécurité, les intervenants se sont efforcés de décortiquer les problèmes majeurs qui émergent dans notre société de plus en plus numérisée. Ils ont sondé les méandres de cette fusion technologique, examinant de près les enjeux et les solutions, les opportunités et les menaces. Cette réunion virtuelle avait pour vocation d'éclairer les participants sur l'évolution de nos relations avec le numérique, qu'il s'agisse de notre perspective individuelle, de celle des organisations, ou de celle des États.

Contexte et Intervenants :

Pour aborder ce sujet complexe, la conférence a fait appel à l'expertise incontestée de la professeure Solange Ghernaouti, membre de l'Université de Lausanne et de l'Académie suisse des sciences. Celle-ci est reconnue pour sa capacité à tisser des liens entre les avancées technologiques, les besoins en matière de sécurité et les solutions de cybersécurité, tout en élargissant son regard du particulier au global. La professeure Ghernaouti avait déjà animé des sessions lors des "Lundi de la Cybersécurité" en 2022 et 2021, explorant des sujets cruciaux tels que l'efficacité de la cybersécurité et le cyberpouvoir.

Au cours de cette conférence, la professeure Ghernaouti a partagé son expertise en se penchant sur l'impact de l'IA sur la cybersécurité. Elle a exploré en détail les risques, les menaces, les opportunités, et a établi des ponts entre les aspects techniques et managériaux, tout en les mettant en perspective avec les évolutions sociétales.

De plus, la conférence a accordé quelques minutes à Cédric Cartau, RSSI et DPO du CHU de Nantes. Il a partagé des informations précieuses sur le Club ISO 27001 de la Région Nantaise, qui réunit des acteurs et des professionnels intéressés par les normes ISO 27000. Cédric Cartau a expliqué la mission du club et répondu aux questions des participants, mettant en avant l'importance de la sécurité de l'information.

La session s'est conclue par une séquence de questions-réponses, permettant aux participants de dialoguer avec la professeure Solange Ghernaouti et Cédric Cartau pour approfondir leur compréhension des thèmes explorés au cours de cette conférence passionnante et actuelle.

I. Constats sur la cybersécurité : dépendance et interdépendance

La première partie de la conférence se concentre sur des constats essentiels concernant la cybersécurité et les problématiques d'intelligence artificielle, mettant en lumière la dépendance croissante et l'interdépendance omniprésente dans notre société numérique en constante évolution.

La dépendance au numérique est un fait indiscutable selon la professeure Ghernaouti. Les services numériques ont envahi nos vies quotidiennes, influençant nos pratiques et nos interactions. Toutefois, cette dépendance aux avantages du monde numérique s'accompagne d'une nouvelle dépendance, à savoir notre dépendance vis-à-vis des fournisseurs de ces services. Cette réalité soulève une question centrale : comment maîtriser ces dépendances ? Cela suscite des préoccupations liées à la souveraineté sur les données et les services numériques.

Un autre constat crucial est l'émergence de nouvelles formes de conflits dans le cyberespace. La cybersécurité ne se limite plus à une question technique ; elle est devenue un enjeu politique, économique et social majeur. Ces nouvelles formes de conflictualité, notamment liées à la cyber influence, sont désormais indissociables de l'intelligence artificielle. Elles affectent non seulement les individus, mais aussi les organisations et les États.

La cybersécurité, autrefois principalement abordée du point de vue technique, dépasse désormais ces limites pour englober des aspects politiques, économiques et sociaux. L'interdisciplinarité est devenue essentielle pour répondre à ces nouveaux défis, mais les frontières académiques traditionnelles entravent cette transition. Former des experts en cybersécurité nécessite une compréhension transversale des risques, du management et de la technologie.

Les défis de la cybersécurité engendrent également des problèmes juridiques, notamment en ce qui concerne la gestion des données et le cloud computing. La dépendance technologique à des fournisseurs étrangers soulève des questions quant à la maîtrise du cadre juridique dans lequel ces données sont traitées.

L'interdépendance est un autre aspect complexe et moins visible de la cybersécurité. Des chaînes de sous-traitance mal maîtrisées peuvent provoquer des fuites de données et des cyberattaques qui touchent des entreprises sous-traitantes, ce qui n'est souvent pas apparent pour les utilisateurs finaux. Cette complexité résultant de l'interdépendance complexe crée un défi de taille pour la maîtrise des risques.

L'approche purement technologique de la cybersécurité se révèle insuffisante. La course à la technologie pour résoudre les problèmes de cybersécurité peut aggraver la situation en introduisant davantage de complexité. Une approche holistique, basée sur la gestion des risques, s'impose pour faire face aux défis actuels de la cybersécurité.

En résumé, cette première partie de la conférence met en lumière la complexité croissante de la cybersécurité et souligne l'importance d'une approche interdisciplinaire pour aborder les risques et les défis. Elle met également en évidence la nécessité de repenser la cybersécurité dans un

monde numérique en constante évolution, en se concentrant sur la maîtrise des dépendances et des interdépendances qui caractérisent notre société contemporaine.

II. Les changements induits par l'ère du numérique

Dans cette deuxième partie de la conférence, l'oratrice souligne les changements significatifs induits par l'ère du numérique. Au cours des dernières décennies, le paysage informatique a été profondément modifié, passant d'un réseau décentralisé et distribué à un environnement centralisé et fortement concentré entre les mains de quelques acteurs hégémoniques, souvent étrangers. Ce phénomène a conduit à une inversion de la distribution du pouvoir et de la sécurité dans le domaine numérique.

Le principal changement réside dans la montée en puissance des plateformes numériques. Ces plateformes ont centralisé non seulement la distribution, mais aussi la transmission, le traitement et la sauvegarde des données, créant ainsi une dynamique de concentration de pouvoir. Cette centralisation s'est traduite par la perte de contrôle sur les données, les traitements et la sécurité, définissant ainsi ce qu'elle appelle l'ère des plateformes.

Le problème majeur réside dans le fait que cette centralisation favorise l'espionnage et impose des comportements et des pratiques qui échappent au contrôle des utilisateurs. Il s'agit d'une logique de soumission et de dépendance, rappelant l'analogie avec le colonialisme numérique. Dans cet environnement, la question essentielle est de savoir quelle marge de manœuvre il reste en matière de cybersécurité.

Un autre aspect préoccupant concerne les entités commerciales qui offrent des services numériques. Leurs intérêts économiques peuvent parfois entrer en conflit avec les intérêts particuliers, voire nationaux, des utilisateurs. La priorité de ces entités est souvent la rentabilité, ce qui peut ne pas être aligné sur la sécurité et la souveraineté nationale.

L'introduction de modèles économiques tels que le cloud, les data centers et l'atomisation des plateformes a renforcé la dépendance, puisque de plus en plus de services sont externalisés. Les utilisateurs paient des loyers pour accéder à leurs propres données, ce qui crée une dépendance aux tarifs imposés par les fournisseurs, introduisant ainsi une forme d'asservissement.

En résumé, cette partie de la conférence met en lumière la centralisation du pouvoir et la perte de contrôle résultant de l'ère des plateformes, ainsi que les conséquences de la dépendance aux acteurs hégémoniques. Elle soulève des questions essentielles concernant la compatibilité des intérêts économiques et des intérêts nationaux, tout en encourageant une réflexion sur la souveraineté et la maîtrise dans le domaine de la cybersécurité.

III. Que peut faire la cybersécurité dans ce contexte ?

Dans cette troisième partie, l'accent est mis sur le rôle de la cybersécurité dans un contexte complexe et en constante évolution. La conférence explore la possibilité d'atteindre certains objectifs grâce à des techniques spécifiques de cybersécurité. Cependant, il est souligné que répondre à ces objectifs n'est pas suffisant.

L'infrastructure numérique est structurée en trois niveaux. Tout d'abord, il y a l'infrastructure matérielle, qui soulève la question de la maîtrise de la chaîne de fabrication et du cycle de vie de ces infrastructures matérielles. De plus, il est mentionné que la cybersécurité doit aborder la problématique de l'Internet des objets, qui permet le contrôle à distance des entités au niveau matériel et logiciel.

Le deuxième niveau est l'infrastructure logicielle et de services, qui est vulnérable aux cyberattaques. Il est question de la nécessité de repenser l'utilisation d'infrastructures vulnérables dans la mise en œuvre du numérique.

Le troisième niveau, l'infrastructure informationnelle, concerne l'utilisation des données avec des infrastructures logicielles et matérielles. Cette partie de l'infrastructure pose des problèmes liés à la profusion d'informations, à la création de contenus et à la collecte de données. La notion de "surface d'attaque" est évoquée, soulignant que plus on se connecte, plus on devient vulnérable aux cyberattaques. La conférence remet également en question le contrôle de cet espace informationnel, qui semble être en grande partie aux mains d'acteurs malveillants.

IV. Qui maitrise les risques ?

Dans cette quatrième partie, l'attention se porte sur la problématique de la maîtrise en cybersécurité, de la mobilité et de la géolocalisation. Plusieurs aspects clés sont abordés :

La remise en question de la maîtrise effective de la cybersécurité. Bien que le chiffrement puisse encore fournir un certain niveau de contrôle, l'opacité des codes propriétaires pose problème. La professeure Ghernaouti suggère la nécessité de reprendre le contrôle sur les environnements, les services et les données pour contrer la dépendance actuelle.

La collecte de données est identifiée comme un enjeu majeur. Elle est désormais au cœur du 21e siècle, notamment grâce au Big Data. Les acteurs hégémoniques ont pris de l'avance dans la collecte de données massives, suscitant des préoccupations quant à la maîtrise de ces données et à leur utilisation pour développer des intelligences artificielles.

La géolocalisation et la mobilité des objets et des individus sont examinées de près. La professeure souligne que la maîtrise de la géolocalisation équivaut à la maîtrise du mouvement, ce qui a des implications significatives. La géolocalisation soulève des questions stratégiques et commerciales, ainsi que des problèmes éthiques et de sécurité liée à la prédiction des comportements des individus.

Enfin, les enjeux géostratégiques sont évoqués, notamment en relation avec la conquête de l'espace et l'implication croissante d'acteurs privés dans l'infrastructure satellitaire. Cette nouvelle dimension de l'espace est perçue comme un domaine essentiel pour la préservation des intérêts stratégiques.

Ainsi, la conférencière met en évidence l'importance de maîtriser la cybersécurité, la collecte de données, la géolocalisation et les enjeux géostratégiques pour préserver les intérêts des individus, des organisations et des nations. Elle suggère qu'il existe des pistes pour aborder ces questions complexes, notamment dans le domaine de la sécurité de l'information et du renseignement.

V. Une rupture civilisationnelle

Dans cette partie, l'accent est mis sur la notion de rupture civilisationnelle provoquée par la captation des données et le pilotage de la société par les techniques d'intelligence artificielle. L'oratrice souligne que nous sommes en train de construire un nouveau modèle de société, où nous sommes essentiellement pilotés par des données, ce qui permet à des fournisseurs de solutions informatiques de concevoir notre réalité sociétale.

L'idée d'un "colonialisme numérique" est évoquée, où les individus deviennent des systèmes d'information, des entités pilotées à distance, susceptibles d'être améliorées par des données. Cette réalité contribue à la perte progressive d'indépendance et de souveraineté.

La convergence des mondes cyber et physique est explorée, ainsi que la complexité qui en découle. Les implications géostratégiques, la transparence croissante des individus et l'opacité grandissante des algorithmes sont également discutées.

L'oratrice soulève des questions sur la pertinence de la confiance dans un environnement numérique caractérisé par l'invisibilité, la traçabilité et la surveillance de masse. Les intérêts économiques sont mis en avant, souvent au détriment de la sécurité.

En fin de compte, il est noté que nous utilisons des solutions numériques qui sont de véritables boîtes noires, ce qui rend la maîtrise de la sécurité difficile, notamment sur l'ensemble du cycle de vie des solutions.

VI. Le code et l’information : des armes de destruction massive ?

La sixième partie aborde la question de savoir si le code informatique et l'information sont devenus des "armes de destruction massive". Elle souligne la dualité de ces outils numériques, qui peuvent être utilisés à la fois pour des cyberattaques destructrices et pour influencer les opinions. Le Big Data est également mentionné comme une forme d'arme de destruction massive.

L'impact de la cyber influence, notamment via les réseaux sociaux, est mis en avant, et il est affirmé par la professeure que la perception et l'influence sont devenues plus importantes que les faits et la réalité. La notion de guerre informationnelle est abordée, soulignant l'importance stratégique de la maîtrise de l'information et de la réputation.

La section évoque ensuite la question de l'interdépendance entre l'énergie, l'électricité et le numérique, soulignant l'importance de la disponibilité des infrastructures numériques. La consommation énergétique du numérique est mise en avant, ainsi que les émissions de gaz à effet de serre associées, en soulignant le besoin croissant d'électricité pour soutenir la croissance exponentielle du numérique. La sobriété numérique est présentée comme une piste pour maîtriser ces risques.

L'impact géopolitique de l'extraction de ressources pour la fabrication d'appareils électroniques est abordé, mettant en évidence les enjeux liés aux ressources naturelles et à l'équité dans la répartition des ressources. Enfin, cette partie souligne la nécessité de lier les problématiques de cybersécurité à celles de l'écologie numérique, en raison de l'impact environnemental de la

consommation numérique, et évoque le concept du jour du dépassement de la Terre en lien avec ces questions.

VII. Une partie du problème : l’obsolescence programmée

La septième partie de la présentation aborde la question de l'obsolescence programmée, qui s'applique non seulement aux matériels et aux logiciels, mais aussi aux êtres humains. L'oratrice pose des questions sur la manière dont l'intelligence artificielle et la transformation numérique affectent la perception de la réalité et de la vérité. Elle souligne que la réalité est de plus en plus médiatisée par le code informatique et que la vérité est devenue malléable grâce à la manipulation des données numériques.

Elle fait référence à la notion de "post-vérité" et suggère que les systèmes d'intelligence artificielle contribuent à cette transformation numérique de la vérité. Elle souligne que la société dépend de ces systèmes basés sur des modèles et des simulations de la réalité, tout en notant que la qualité des données et la sécurité posent des problèmes en raison du caractère opaque de ces systèmes.

L'oratrice évoque également l'idée de la "performance" comme étant au cœur de ces systèmes, et souligne que l'optimisation peut souvent se faire au détriment de l'humanité. Elle met en garde contre la difficulté croissante de distinguer le vrai du faux dans un environnement numérique déstabilisant, et souligne la culture de la fausse information qui prévaut, notamment sur les réseaux sociaux.

Elle conclut en évoquant la transformation des humains en machines, contraints de penser de manière binaire, et la naissance d'un nouveau régime de vérité dans lequel le débat est souvent confisqué.

VIII. L’intelligence artificielle, un processus de confiscation ?

Dans la huitième et dernière partie de la présentation, l'oratrice soulève la question de savoir si les solutions basées sur l'intelligence artificielle entraînent un nouveau régime de vérité. Elle se demande si l'intelligence artificielle ne confisque pas progressivement le libre arbitre des êtres humains, car nos décisions et actions sont de plus en plus influencées par des logiciels. Elle met en avant la nécessité de maîtriser les risques liés à ces technologies pour pouvoir profiter de leurs avantages, tout en évoquant la perte de savoir-faire humains au profit de systèmes informatiques.

Elle mentionne également les défis liés à la dépendance croissante aux technologies, aux risques systémiques, et à la complexité de la société actuelle. L'oratrice propose de réfléchir à une "retenue numérique" plutôt que de poursuivre une fuite en avant technologique, tout en se réappropriant notre libre arbitre et nos valeurs partagées.

Elle conclut en abordant l'idée de "techno-optimisme" en opposition au déni des risques technologiques, et en soulignant l'importance de prendre conscience des risques liés à la finitude des ressources planétaires. Elle invite à repenser la recherche de croissance et de performance économique à tout prix, et à envisager l'héritage que nous laisserons aux générations futures.

La professeure Ghernaouti finit son intervention en remerciant l'audience et en présentant ses deux derniers ouvrages, dont l'un traite de la cybercriminalité et de la cybersécurité.

IX. Intervention de Cédric Cartau

L'intervention de Cédric Cartau portait sur la création récente d'une antenne nantaise du Club ISO 27001, en collaboration avec Mickaël Ferton de la société DIGITEMIS. L'objectif principal de cette antenne est de promouvoir la norme ISO 27001 dans la région et d'organiser des conférences thématiques axées sur le contenu, sans intention de favoriser la promotion commerciale.

Le club vise à rassembler divers profils, qu'il s'agisse d'entreprises utilisatrices ou de prestataires, dans le but de fournir des informations et de stimuler le partage d'expériences. Le périmètre géographique des participants est en cours de définition, mais pour l'instant, il est ouvert à tous, même à ceux de l'extérieur. Les réunions se tiennent environ trois à quatre fois par an, soit en présentiel, soit en mode mixte (présentiel et à distance). Les conférences abordent divers sujets, notamment des retours d'expérience, des cas d'usage, des problèmes rencontrés dans la mise en œuvre de la norme, etc.

Cédric Cartau invite tous ceux qui souhaitent participer ou en savoir plus à prendre contact avec lui ou avec Mickaël Ferton pour l'inscription. La cotisation pour adhérer au club national ISO 27001 est de 27 euros par personne et par an. Actuellement, le club compte plus d'une cinquantaine de membres.

X. Séance de questions / réponses

Question 1 :

Pour garantir la protection et la confidentialité des données en utilisant l’IA générative, quel est votre regard sur la solution souveraine proposée par Docaposte ?

Solange Ghernaouti estime qu'une manière de garantir la protection et la confidentialité des données tout en utilisant l'IA générative est de disposer de la capacité de développer ses propres modèles d'IA générative en open source et de maintenir les données en local. Cela constituerait une réappropriation des logiciels et des données. Cependant, l’oratrice souligne que cette solution souveraine, telle que celle proposée par Docaposte, pourrait être une bonne idée pour répondre aux besoins spécifiques d'un environnement particulier, à condition que l'entité dispose des compétences nécessaires pour développer et maintenir cette solution. Elle précise également que certaines grandes entreprises investissent dans la construction de leurs propres mini-centrales nucléaires pour garantir une alimentation énergétique suffisante pour leurs besoins, soulignant ainsi l'importance de reprendre le contrôle des ressources nécessaires à la performance. Cependant, elle mentionne que cette approche pourrait être limitée à quelques acteurs, à condition que les données et les compétences soient disponibles et maîtrisées.

Question 2 :

Faut-il une opération sévère, vigoureuse, de hiérarchisation des fonctions supportées par le “numérique” ?

La réponse à la question de savoir s'il faut entreprendre une opération sévère de hiérarchisation des fonctions supportées par le numérique met en avant l'importance de prioriser les usages du numérique. L'oratrice souligne que cela est crucial, notamment en cas de crise, pour s'assurer que le numérique soit réservé aux tâches strictement nécessaires. Cela permettrait de regagner le contrôle sur les environnements numériques et d'aborder la question écologique. Elle estime que de nombreuses applications sont davantage axées sur le divertissement que sur la nécessité, et met en lumière les dépendances et les phénomènes d'addiction qui ont émergé. L'oratrice s'inquiète de l'impact sur la société, où les gens sont de plus en plus absorbés par leurs écrans, même au détriment des interactions sociales. En fin de compte, elle considère que pour maîtriser les ressources limitées, y compris dans le domaine numérique, il est impératif de repenser la priorisation des usages. Cependant, elle reconnaît que cela peut être une démarche douloureuse nécessitant une vision, une stratégie, un plan d'action et une volonté politique. L’intervenante insiste sur la nécessité d'aller au-delà de la fuite en avant technologique et de se concentrer sur la sécurité.

Question 3 :

Quelles sont les instances à créer afin de résoudre la problématique précédente ?

La réponse de la professeure suggère qu'il existe une croyance en France et en Suisse selon laquelle l'innovation numérique est la solution à de nombreux problèmes. Cependant, l'oratrice soulève le dilemme d'une société de plus en plus numérique tout en imposant des exigences contradictoires, comme l'exigence d'avoir un téléphone pour prendre un billet de bus. Elle se demande qui devrait décider de l'usage raisonné des technologies et des solutions numériques (LUCAS) et affirme que ce ne devrait pas être la responsabilité des fournisseurs de solutions ni des géants de la technologie, ni même de certains politiques qui ne comprennent peut-être pas entièrement les problèmes. L’oratrice suggère que la société pourrait commencer à repenser ses besoins en technologies numériques lorsque les défis et les inconvénients deviendront insupportables. Pour l'instant, elle considère que nous n'avons pas encore atteint ce point.

Question 4 :

Beaucoup de logiciels métiers DPO sont étrangers, n’est-ce pas un risque ?

L'utilisation de logiciels métiers DPO étrangers présente un risque important en termes de souveraineté, car il y a un manque de maîtrise du cadre juridique associé à ces solutions. Cette situation crée un risque juridique majeur, car les lois extraterritoriales peuvent s'appliquer, et il est difficile de contrôler à la fois les technologies et le cadre juridique dans lequel elles opèrent. En fin de compte, l’oratrice exprime des doutes sur la capacité à maîtriser efficacement ces facteurs dans ces conditions.

Question 5 :

Faudrait-il plus de pouvoir aux associations de consommateurs ?

Il est suggéré qu'une augmentation du pouvoir des associations de consommateurs pourrait être bénéfique. De plus en plus de consommateurs prennent conscience des risques et des coûts qui leur incombent en raison de la transition vers le tout numérique. Cette prise de conscience au niveau individuel pourrait contribuer à une prise de conscience plus large du problème, qui pourrait entraîner une résistance accrue au passage au tout numérique. Ce phénomène est parallèle à d'autres zones de résistance, notamment dans le domaine de la chimie, car les enjeux sont similaires.

Question 6 :

Comment la cybersécurité peut-elle apporter une solution à la qualité des données ?

La cybersécurité seule ne peut pas garantir la qualité des données, car même si les mécanismes de cybersécurité sont en place pour protéger les données, la qualité des données à la base reste un problème. Il est souligné que la vérification de la qualité des données est un processus distinct. Les normes de qualité des données ont été quelque peu négligées par rapport aux normes de sécurité de l'information. La qualité des données dépend également de ce qui est capturé dans les données, ce qui est conservé et ce qui est rejeté. La qualité des données est comparable au concept de médicaments conçus pour une population spécifique, pas pour tout le monde.

Question 7 :

Avez-vous des ressources scientifiques pour corroborer vos dires et vos pensées ?

L'intervenante affirme qu'il existe des ressources scientifiques pour soutenir ses points de vue, mais elle reconnaît que ces idées ne sont pas isolées et partagées par d'autres chercheurs. Cependant, elle souligne que le financement de la recherche dans ces domaines peut être difficile à obtenir, en partie parce que les fonds proviennent souvent des acteurs hégémoniques. De plus, les lignes directrices de recherche sont parfois influencées par des organisations telles que le World Economic Forum. Elle soulève également la préoccupation selon laquelle de grandes entreprises proposent du matériel et des services gratuits aux écoles et aux universités, contribuant ainsi à façonner les comportements des jeunes générations en matière de numérique.

Question 8 :

Quel sera l’impact du DSA ?

La professeure Ghernaouti critique l'impact du Digital Services Act (DSA) en soulignant que certaines initiatives visant à réglementer le numérique manquent de pluralité des acteurs et des visions. Elle mentionne que des initiatives comme "For Good Intelligence Artificielle" et "Cyber For Good" sont portées par des acteurs tels que le Boston Consulting Group, ce qui peut freiner une élaboration de pensée plus diversifiée. Elle s'inquiète du fait que malgré les directives européennes, le problème persiste, car les utilisateurs continuent de fournir leurs données aux géants du numérique, y compris leurs données de santé. Elle plaide en faveur de

soutenir les initiatives de développement local plutôt que de confier la maîtrise et les financements aux acteurs économiques déjà bien établis.

Question 9 :

Sachant que nous utilisons de plus en plus de d'outils, comment pouvons-nous préconiser une sobriété numérique ?

L'intervenante aborde la question de la sobriété numérique en soulignant que la réponse dépendra des contextes et des pratiques. Elle suggère que, dans certaines situations, il est possible de privilégier des solutions locales plutôt que d'adopter des outils numériques étrangers. Elle donne l'exemple du piratage de données génétiques de la société "Twenty Three and Me" et met en avant l'importance de soutenir et d'adopter des logiciels et solutions numériques développés localement, contribuant ainsi à la souveraineté numérique. Elle remet en question les discours sur la souveraineté numérique, mentionnant que de nombreuses régions n'ont pas encore atteint cette souveraineté, et suggère d'adopter des attitudes en conséquence plutôt que de faire semblant de la posséder.

Question 10 :

L’homme ne pourra pas tout contrôler. Pour vérifier la qualité des données, pourra-t-on faire confiance à l’IA ?

L'intervenante souligne que la dépendance croissante à l'IA soulève des questions sur la confiance. Elle remet en question la tendance à la confiance aveugle dans l'IA et suggère que la confiance en l'IA dépendra de l'engagement des fournisseurs d'IA envers la responsabilité. Elle estime que les fournisseurs devraient assumer la qualité, la fiabilité et la résilience de leurs produits plutôt que de faire peser les risques sur les utilisateurs et les entreprises. Elle met en avant l'importance de responsabiliser les acteurs qui produisent des solutions d'IA pour instaurer une plus grande confiance dans ces technologies.

Question 11 :

Quelles sont les tendances informatiques qui devraient dominer 2024 ?

L'intervenante évoque les préoccupations concernant la centralisation des données dans les fournisseurs de Cloud et suggère qu'il est nécessaire de repenser l'architecture d'interconnexion pour distribuer les risques. Elle insiste sur l'importance de savoir à qui appartiennent les logiciels manipulant les données et plaide en faveur de l'enseignement de l'open source. Elle souligne que la sécurité dépend de la nature des logiciels utilisés pour accéder aux données, que ce soit en local ou dans le Cloud. Elle mentionne également la question de la confiance envers les acteurs privés ou publics, ainsi que la balkanisation de l'Internet en raison de tensions géopolitiques. En ce qui concerne les tendances informatiques pour 2024, elle évoque la prolifération des objets connectés et la prise de conscience de la criticité des informations de santé, mais admet ne pas avoir de réponse claire à cette question.

Question 12 :

L’historisation des données chiffrées d’aujourd’hui permettra-t-elle demain de les décrypter avec les ordinateurs quantiques ? Est-ce un risque vraisemblable ?

La réponse à la question sur l'historisation des données chiffrées et les ordinateurs quantiques souligne l'importance du chiffrement pour la sécurité des données. L'intervenante suggère que les ordinateurs quantiques représentent un défi potentiel pour la sécurité des données chiffrées et encourage à investir dans le chiffrement, y compris le chiffrement post-quantique, pour maîtriser ces enjeux. Elle met également en avant l'importance de la mise en œuvre du chiffrement pour éviter les vulnérabilités liées à la numérisation des données.

Question 13 :

Ne pensez-vous pas que le retour en arrière que vous préconisez n'entraine un retour en arrière sur les progrès scientifiques et notamment médicaux ?

La professeure Solange Ghernaouti répond à la question concernant le retour en arrière sur les progrès scientifiques, notamment médicaux, en précisant qu'elle ne préconise pas un retour en arrière, mais plutôt un numérique raisonné et raisonnable. Elle suggère que les progrès scientifiques pourraient être préservés en construisant des systèmes respectueux des droits des personnes, tout en priorisant des actions essentielles au détriment de divertissements numériques gourmands en ressources. Elle souligne le manque de débats de société sur ces questions et l'absence de stratégie et de plan d'action cohérent pour l'utilisation du numérique.

Conclusion

La conférence a abordé de nombreuses questions liées à la cybersécurité, la protection des données, la souveraineté numérique, et les implications des avancées technologiques. La professeure Solange Ghernaouti souligne la nécessité d'adopter une approche raisonnée et raisonnable du numérique plutôt que de céder à une dépendance à la technologie. Elle met en avant des inquiétudes concernant la perte de contrôle sur nos données, l'impact des IA, et les enjeux de sécurité. Elle encourage également une réflexion plus profonde sur l'évolution de notre utilisation du numérique et la préservation des droits des individus.

Selon moi, cette conférence soulève des préoccupations pertinentes concernant la protection des données, la dépendance aux technologies du numérique, et la nécessité de repenser notre approche de la cybersécurité. Il est important de trouver un équilibre entre les progrès technologiques et la protection de la vie privée, tout en encourageant une réflexion plus large sur l'impact sociétal des avancées technologiques. La souveraineté numérique est également un sujet crucial, et il est essentiel que les débats de société et les stratégies cohérentes guident nos actions dans ce domaine.