Quelles technologies pour assurer la confiance numérique ?

Anonymat, confidentialité, traçabilité souveraine

Internet, Cloud, IA générative, voiture connectée, autant de cauchemars pour la protection de vos données personnelles sensibles. Votre santé, vos origines, votre patrimoine génétique, vos goûts musicaux, vos habitudes de déplacement, votre vie devient transparente pour les marchands de données, et toutes les dérives deviennent possibles. Fort heureusement, des technologies respectant la vie privée et le secret des affaires existent, mais elles sont mal connues et peu employées.

Entre l'IA et la blockchain, le numérique a vécu beaucoup de changements profonds ces dernières années. En quoi manque-t-il de la « confiance » pour développer tout un séminaire sur ce sujet ?

David Menga : Il est vrai qu'il y a beaucoup de nouveaux sujets sur le numérique. Tout le monde parle d'intelligence artificielle, de monnaie numérique, d'utilisation de la blockchain… Mais on oublie joyeusement les questions de respect de la vie privée, de confidentialité. Et c'est d'autant plus embêtant que ces technologies absorbent énormément d'informations personnelles pour être plus efficace. Toutes ces données, si elles ne sont pas protégées, peuvent devenir visibles et accessibles à n'importe qui, et produire des effets de bord néfastes. Prenons le cas particulier des données de santé : votre assureur porte sur elles un regard différent du votre… Idem pour votre vie privée, vous ne voulez pas que vos voisins sachent tout ce qu'il se passe chez vous. Ou qu'ils connaissent votre état de santé. Idem avec vos origines, votre patrimoine génétique, vos goûts musicaux, vos habitudes de déplacement… Votre vie devient transparente pour les marchands de données.

Vous pensez réellement qu'il y a un souci sur la protection des données ?

Nous vivons un développement exponentiel des technologies de type IA et blockchain - durant le séminaire nous traiterons davantage des IA génératives, car elles ont besoin de bien plus de données pour devenir performantes. Ce développement est un fait. Mais nous avons beaucoup d'exemples depuis un an de défauts de protection des données. En parallèle, nous sommes dans un contexte de croissance extrêmement forte des cyberattaques. Tout cela pose des problèmes. Avant tout, il faut des

garde-fous. Mon propos consiste à dire qu'on doit assurer la confidentialité de certains types de données, en amont, indépendamment des garde-fous règlementaires. Nous devons sortir des effets de manche répétés sur la sécurité, pour enfin passer aux choses concrètes. Et les solutions existent.

Cela concerne toutes les données ?

Deux catégories sont plus sensibles : les données à caractère privé et les données d'entreprises. On l'oublie souvent, mais toute la matière grise créée par les entreprises doit aussi être protégée. Ces deux domaines, au bout du compte, sont ceux qui cristallisent la perte de confiance dans le numérique. Et sans confiance, pas de business. C'est la base des échanges commerciaux. Si le numérique et plus particulièrement ces technologies veulent croître, il nous faut progresser là-dessus. Alors comment est-on capable d'assurer l'anonymat des personnes ? La confidentialité des échanges ? Comment garantir la traçabilité des informations ? Lorsqu'on livre une information à quelqu'un, on doit savoir où elle finit. Surtout si cela concerne ma santé… Et clairement, on peut dire ce sont les journées « portes ouvertes », pour certaines plateformes, à l'heure actuelle, sur les données personnelles : on ne sait absolument pas ce qu'elles en font. Nous n'avons aucune idée sur le devenir de nos données. Alors que la définition même de la vie privée, c'est de savoir à qui vous confiez vos secrets !

Selon vous, nous n'avançons pas assez vite… Mais est-ce seulement possible ? La technologie existe-t-elle ?

Oui. Les solutions existent, et nous les occultons. Quand Christine Lagarde, la présidente de la banque Centrale Européenne, affirme que la monnaie numérique est un problème parce que la blockchain ne garantit pas l'anonymat, mais seulement le pseudonymat, et qu'en conséquence, elle n'offre pas les mêmes garanties que les espèces tout court, il faut s'interroger sur la véracité de cet argument, et sur les conséquences de telles déclarations. Car une blockchain, certes, fonctionne sur le mode pseudonymisé, mais peut être rendue anonyme. Et nous le verrons pendant le séminaire avec les solutions comme Monero, ou Zcash. Ce n'est donc pas une question de faisabilité technique, mais de volonté politique. On utilise la blockchain comme paravent au développement de la monnaie numérique. Pourtant le politique a des équipes techniques à disposition, il pourrait avancer s'il le voulait.

Idem pour la question de la vie privée. C'est un droit reconnu par la déclaration des droits de l'homme. Ce n'est pas une vue de l'esprit, théorique. C'est très concret, la vie privée. Personnellement, je prétends qu'il faut étendre le droit des humains du monde réel dans le numérique. Et des solutions existent. Il est possible d'améliorer l'anonymat en ligne. Et ce séminaire sera l'occasion de le prouver, de discuter de leurs degrés d'applications et de leurs limites. Nous entrerons en profondeur dans les domaines de la santé et du marketing, qui sont deux secteurs qui posent des questions dans le recueil des données pour construire les modèles d'IA. Mais des technologies respectant la vie privée et le secret des affaires existent, mais elles sont mal connues et peu employées.

Mais les exemples qui seront développés pendant le séminaire, sont-ils viables ? Sont-ils déjà implémentés ?

Oui. Les solutions sont déjà implémentées. Pour l'anonymisation des données de santé, des CHU utilisent déjà des solutions. Certains seulement, car tous n'ont pas les mêmes politiques ou les mêmes moyens. Mais l'anonymisation fonctionne : pour vérifier l'efficacité des traitements thérapeutiques, vous n'avez pas besoin des noms des patients. Car dans le cadre de la médecine statistique, nous traitons des pathologies, pas des patients. Bien sûr, il faut ensuite du soin, de la considération et de l'empathie pour faciliter la guérison, mais ce n'est pas le domaine de la médecine statistique. Les statistiques, d'ailleurs, sont nées avec les épidémies, pour les comprendre et mieux les éradiquer.

Comment faire pour que le grand public comprenne l'importance du sujet ?

Tout d'abord, il faut s'assurer que le travail soit bien fait. Pour cela, il faut mettre dans le cahier des charges de la solution que les données ne quittent pas l'hôpital. En réalité, vous n'avez pas besoin qu'elles sortent de l'endroit où elles sont stockées. Ensuite, pour parler au grand public, il faut parler que quelque chose qu'il connait. Par exemple, un coffre-fort, quand vous y mettez des documents, ils ne quittent pas la banque. Eh bien cela doit être pareil avec les données : elles ne quittent pas l'hôpital.

Mais comment faire pour qu'il prenne conscience des enjeux pour lui ?

La prise de conscience fonctionne beaucoup par scandale. Lorsque quelqu'un pirate votre ordinateur, vous comprenez bien vite l'importance de la sécurité. Sur internet, on ne se rend compte de rien car tout paraît fluide et simple. Et depuis la création du web, les données sont le prix à payer, contre la gratuité. Mais cela ne doit pas empêcher d'établir des protections à la racine des systèmes. Lorsqu'on sort sans se couvrir alors qu'il pleut, on le fait en toute conscience, en sachant qu'on peut tomber malade. On connaît le risque. Eh bien cela doit être pareil avec le monde numérique. Nous devons apprendre à l'utiliser, et connaître les risques associés. Nous avons besoin de transparence de la part des plateformes, et globalement de tous les acteurs du numérique, afin de pouvoir l'utiliser et le développer en toute confiance.

Lien vers la présentation et le programme du séminaire :
https://www.association-aristote.fr/evenements/seminaire-quelles-technologies-pour-assurer-la-confiance-numerique/