TechnoVision?: Les 5 tendances technologiques à suivre en 2027

Capgemini dévoile aujourd'hui son « Top 5 TechnoVision des tendances technologiques à suivre en 2027 », qui met en lumière les technologies qui devraient atteindre un point d'inflexion l'année prochaine. Alors que les entreprises cherchent à gagner en autonomie dans leurs processus et leurs opérations, l'IA entre dans une nouvelle ère?: elle a dépassé le rôle d'« assistant » pour former des systèmes capables d'agir par eux-mêmes et d'exécuter des tâches. En 2027, cette évolution transformera les opérations des entreprises, la cybersécurité, la R&D et le commerce, créant de nouvelles opportunités tout en créant de nouveaux enjeux en matière de gouvernance, de sécurité et de résilience.

« L'an dernier, le Top 5 des tendances technologiques de Capgemini mettait en lumière l'intégration croissante de l'IA dans les architectures d'entreprise, le développement logiciel et les opérations, explique Pascal Brier, Directeur de l'Innovation de Capgemini et membre du Comité Exécutif du Groupe. *Avec des agents d'IA capables d'agir de manière autonome, l'IA franchit aujourd'hui un nouveau cap. En 2027, le principal défi pour les organisations sera de déployer cette autonomie à grande échelle sans pour autant perdre le contrôle. Il leur faudra pour cela gérer les interactions entre agents, maîtriser les résultats inattendus et affronter des menaces qui se propagent à une vitesse surhumaine. Au-delà de ces défis, l'IA agentique va transformer en profondeur les méthodes de travail actuelles, qu'il s'agisse d'accélérer l'innovation en R&D ou de réinventer les interactions entre les entreprises et les consommateurs. »*

Les technologies à suivre en 2027 :

1. **Entreprise agentique et systèmes multi-agents?: quand des agents interagissent de manière imprévue**

Aujourd'hui, la plupart des agents d'IA et des systèmes agentiques sont suffisamment simples pour être testés avant leur mise en production. Mais à mesure que leur nombre augmente, il devient impossible de tester l'ensemble de leurs interactions?: par exemple, pour une entreprise qui utilise 15 agents d'IA, cela représente 105 paires d'interactions possibles, alors qu'avec 1?000 agents et 200 systèmes agentiques, ce chiffre atteint près de 720?000. À une telle échelle, les agents pourraient adopter des comportements que personne n'avait anticipés. Chaque agent peut prendre une décision raisonnable au regard de son propre objectif et des informations dont il dispose, mais ces décisions peuvent interagir entre elles, provoquer des réactions chez d'autres agents et, à terme, produire un résultat inattendu à l'échelle du système. Chaque agent peut avoir raison, pourtant le système a tort, avec des conséquences potentiellement graves pour l'entreprise.

Pourquoi c'est important?: Le contrôle devra à l'avenir s'exercer à trois niveaux?: un harnais autour de chaque agent, une tour de contrôle pour chaque système agentique et une tour de contrôle à l'échelle de l'entreprise pour superviser l'ensemble. En 2027, les tours de contrôle des entreprises devront tenir un registre de chaque agent et système agentique, avec une identité et des autorisations propres à chacun, et assurer le suivi des résultats obtenus et de leur consommation de ressources. Elles devront également offrir une visibilité sur les interactions entre agents, fixer des limites à ce qu'ils peuvent réaliser ensemble, et permettre de les arrêter.

2. **L'IA autonome en toute confiance et en toute sécurité?: endiguer sans même comprendre**

Garantir la sécurité de l'IA impliquait jusqu'ici de pouvoir retracer la manière dont elle prend ses décisions, de limiter les accès des agents d'IA et des systèmes agentiques, et de vérifier que chaque décision reste conforme aux règles de l'entreprise. Cette approche est aujourd'hui mise à l'épreuve, car certains nouveaux modèles n'affichent plus comment ils procèdent étape par étape. À mesure que les systèmes d'IA deviennent plus sophistiqués et opèrent à plus grande échelle, il devient donc plus difficile d'en vérifier la totalité du raisonnement. Une IA sûre implique donc d'accepter que des erreurs et des incidents puissent survenir, et de décider jusqu'où leurs conséquences peuvent se propager. Concrètement, cela signifie que les organisations doivent surveiller les signaux d'alerte, qu'il s'agisse d'un agent utilisant un outil non autorisé ou d'un autre

ne respectant pas certaines de ses instructions. Il peut également s'agir d'une hausse soudaine des coûts ou du temps de réponse, ou encore d'un système qui cesse de fonctionner. Lorsque ces signaux apparaissent, l'agent concerné doit être contrôlé ou mis hors service.

Pourquoi c'est important?: En 2027, les organisations devront se concentrer davantage sur leur capacité d'endiguement/de confinement de l'IA que sur son explicabilité. Elles devront également mettre en place des tours de contrôle à l'échelle de l'entreprise, couvrant l'ensemble des agents et des systèmes agentiques, et permettant de surveiller les interactions entre agents ainsi que les premiers signes d'erreurs techniques.

3. **La cybersécurité à l'ère de l'IA?: des cyberattaques lancées à une vitesse surhumaine**

Un agent d'IA peut désormais identifier de manière autonome des failles logicielles et les exploiter pour mener de véritables attaques, sans intervention humaine, et ce même s'il n'a pas été conçu à cette fin. En matière d'attaque, le risque augmente à mesure que l'IA renforce les capacités disponibles pour identifier les vulnérabilités et en tirer parti, notamment des attaques permettant de prendre le contrôle de systèmes critiques. Du point de vue de la défense, la surface d'attaque ne cesse de s'étendre?: chaque assistant d'IA, chaque agent et chaque système agentique déployé crée un nouveau point d'entrée potentiel, et ce alors que les capacités de détection d'intrusions ne progressent pas au même rythme. À mesure que les attaques s'automatisent et s'industrialisent, une cyberdéfense qui attend l'intervention d'un analyste humain a déjà perdu la bataille.

Pourquoi c'est important?: En 2027, alors que les cyberattaques adopteront de plus en plus la vitesse de l'IA, les opérations de sécurité devront évoluer au même rythme. Les centres opérationnels de sécurité devront s'appuyer sur les machines pour trier les alertes et y répondre, tandis que les humains définiront les règles, déploieront les systèmes agentiques et en assureront la supervision. Cela implique également d'évoluer vers une nouvelle génération de centres opérationnels de sécurité, capables de détecter une nouvelle menace en quelques minutes et d'y remédier bien plus rapidement.

4. **R&D agentique?: repousser les limites des capacités de recherche**

Dans la R&D, la capacité à explorer, examiner et valider différentes options a traditionnellement été limitée par les ressources disponibles et les capacités de test. L'IA change la donne à deux étapes clés?: l'exploration, qui consiste à trouver la bonne idée pour un produit, et l'exécution, qui permet de la concrétiser. Dans la phase d'exploration, les organisations ont historiquement été contraintes par le nombre d'options qu'elles pouvaient tester. L'IA permet de dépasser cette limite

en permettant d’explorer un éventail beaucoup plus large de possibilités, qu’il s’agisse de produits moléculaires tels que les médicaments, les produits chimiques et les matériaux, ou de produits physiques comme les véhicules, les machines et les biens de consommation. Dans la phase d’exécution, l’IA intervient à chaque étape, avec des agents capables d’écrire, de tester et de corriger du code, tandis que l’IA joue un rôle croissant dans la conception, la simulation, les tests et la gestion du cycle de vie des produits.

Pourquoi c’est important?: En 2027, l’IA permettra aux organisations d’explorer et d’évaluer un éventail beaucoup plus large d’options, tout en accélérant leur mise en œuvre. Dans la phase d’exploration, elles pourront identifier plus rapidement les pistes les plus prometteuses et mieux les évaluer, notamment dans la découverte de molécules. Dans la phase d’exécution, les ingénieurs seront de plus en plus assistés par l’IA, permettant ainsi de réduire les coûts et les délais de mise sur le marché. Le modèle opérationnel de la R&D devra évoluer autour de l’IA, des agents, des données et des outils conçus nativement pour l’IA.

5. **Commerce agentique?: des agents des deux côtés de la transaction**

Les agents d’IA transforment les deux côtés du comptoir?: l’achat comme la vente. Côté acheteurs, les consommateurs peuvent demander à un assistant d’IA de rechercher des produits selon des critères tels que le prix, la disponibilité et la livraison. En quelques secondes, l’agent peut comparer les informations relatives au produit, au prix ou à la livraison auprès de plusieurs distributeurs. Du côté des vendeurs, les distributeurs commencent à utiliser des systèmes agentiques pour piloter leurs opérations, enrichir leurs catalogues, ajuster les prix et les promotions, réapprovisionner les stocks, et gérer le service client et les retours. Les agents deviennent ainsi rapidement partie intégrante de la transaction elle-même.

Pourquoi c’est important?: En 2027, les organisations devront rendre leurs activités davantage lisibles par l’IA. Cela implique de fournir des données fiables et structurées sur les produits, les prix, les stocks et la livraison, mais aussi de pouvoir authentifier les agents auxquels elles autorisent l’accès et de bloquer les agents malveillants. Du côté des vendeurs, les systèmes agentiques peuvent accroître l’efficacité opérationnelle et accélérer les opérations commerciales. Dans le même temps, alors que l’IA influence de plus en plus la manière dont les consommateurs découvrent, évaluent et achètent des produits, les marques devront à la fois veiller à ce que leurs produits restent visibles et pertinents pour les assistants d’IA, tout en continuant à développer la préférence de marque, la fidélité et la confiance de leurs clients.