smartCIO

Édition EMEA | Une publication Workday | N° 10

Résoudre l'équation de la confiance : l'IA responsable dans la région EMEA

Dans ce numéro :

Scannez le QR code pour voir les numéros précédents :

Édito

Bienvenue dans le dernier numéro de smartCIO, dans lequel nous vous présentons des analyses sur les dernières tendances technologiques, ainsi que les opinions et perspectives régionales des leaders IT de la région EMEA.

Si vous avez suivi les événements du Forum économique mondial de Davos, vous savez que la confiance a été au cœur du rassemblement annuel des dirigeants politiques et économiques du monde entier. Alors que l'IA continue de dominer l'ordre du jour dans les technologies, les médias et les entreprises, les dirigeants doivent relever les défis de la confiance et de l'IA responsable.

Dans ce numéro, nous explorons les raisons pour lesquelles le succès de l'IA dépend de la capacité des leaders de l'IA à gagner la confiance des collaborateurs et à déployer la technologie de manière responsable. Nous nous penchons également sur le rôle plus large de la confiance dans les technologies de l'information et sur la manière dont les entreprises font face à ce défi.

Martin Veitch, un expert IT coutumier des changements technologiques majeurs, nous donne son avis sur la façon dont les leaders IT peuvent remporter la bataille de la confiance.

Ce numéro est aussi l'occasion d'approfondir une nouvelle étude mondiale de Workday qui met en évidence l'existence d'un écart de confiance entre les dirigeants et leurs collaborateurs, et ce sur quoi les leaders devraient se concentrer pour y remédier.

Dans le même temps, Anja Fordon analyse certaines des raisons pour lesquelles l'IA suscite autant d'enthousiasme que de méfiance, au-delà des craintes et du battage médiatique que suscite cette révolution technologique.

Nous consacrons un article à Veolia, client de Workday, dans lequel nous examinons comment instaurer la confiance à une époque marquée par l'insécurité des données.

Enfin, Accenture et KPMG, partenaires de Workday, partagent leurs conseils sur la façon de développer la confiance et l'enthousiasme des collaborateurs en s'appuyant sur une IA responsable et en remédiant au manque de compétences informatiques.

Nous espérons que vous apprécierez ce numéro et qu'il vous sera utile dans votre propre parcours en matière d'IA.

Angelique De Vries-Schipperijn
President EMEA, Workday

Sommaire

Trois raisons d'échanger avec nous

SOUMETTEZ-NOUS vos idées de sujets, **RÉDIGEZ** vos propres articles pour le magazine ou **ABONNEZ-VOUS** pour rejoindre la communauté smartCIO et recevoir l'édition digitale trimestrielle ainsi que des infos sur les événements locaux.

Tout ceci via une seule adresse.

Écrivez-nous à **smartcioemea@workday.com**

À l'ère de l'IA, les dirigeants doivent instaurer la confiance. Mais comment ?

Avec la grande incertitude entourant l'IA, les équipes de sécurité et de gouvernance évoluent dans un environnement en perpétuel changement. Mais une chose est sûre : la confiance n'a jamais été aussi importante.

Par **Martin Veitch**,
Observateur du secteur

Dans le dictionnaire, la confiance est l'« espérance ferme, l'assurance d'une personne qui se fie à quelqu'un ou à quelque chose. » C'est un bon point de départ, mais nous savons tous qu'elle peut être difficile à acquérir. Dès l'enfance, on nous inculque que « la confiance ne se donne pas, mais se gagne ». À l'âge adulte, l'importance de la transparence, de l'honnêteté et de la responsabilisation n'est plus à démontrer. Malheureusement, nous savons aussi de plus en plus à quel point la confiance peut être fragile, facilement rompue et perdue. Nous sommes tous conscients de l'importance de la confiance, particulièrement dans un contexte de changement, sur un terrain peu favorable et inconnu où il faut négocier pour améliorer les choses. Et avec l'IA, les entreprises connaissent le plus grand des changements.

Que signifie la confiance ?

Le fait est que la confiance est un sujet complexe. Paul Thagard, dans *Psychology Today*, l'a qualifiée de « processus neuronal complexe [qui est] rarement absolu, mais [...] limité à des situations particulières [...] la rencontre entre les expériences actuelles, les souvenirs et les concepts ». En d'autres termes, contrairement à Pangloss dans *Candide* de Voltaire, nous ne faisons pas aveuglément confiance à tout le monde. Les circonstances dans lesquelles nous développons notre sentiment de confiance envers quelqu'un et le degré de confiance que nous accordons reposent sur un ensemble d'expériences directes et indirectes vécues tout au long de notre vie. Et lorsque cette confiance est ébranlée, il est très difficile de la restaurer.

Paul J. Zak, dans la *Harvard Business Review*, est allé plus loin en mesurant la production d'ocytocine pour montrer que la confiance peut entraîner des changements positifs spectaculaires au niveau du stress, de l'énergie, de la productivité et de l'engagement. Même sans ces preuves tangibles, la plupart d'entre nous conviendront instinctivement que la confiance est une bonne chose qui conduit à des résultats positifs.

Nous serons peu nombreux à développer nos propres modèles LLM ou à ressentir le besoin de créer des applications centrales sur mesure en dehors de celles offrant un avantage concurrentiel direct. Nous devons donc sélectionner des fournisseurs et autres partenaires ayant de solides antécédents en matière de gestion des données.

Mais, en particulier dans le sillage de la « Grande démission » et de la « Démission silencieuse », tous les dirigeants doivent s'atteler à instaurer la confiance et comprendre pourquoi elle est préférable à des mesures de fidélisation rudimentaires qui donnent le sentiment d'être enfermé dans une « prison dorée ». C'est particulièrement vrai aujourd'hui pour les DSI avec l'IA et le Machine Learning (ML) qui agissent comme des super-catalyseurs, synonyme de changements massifs dans notre façon de travailler.

Le changement est difficile sans confiance

Le changement est l'un des aspects les plus difficiles à gérer dans une entreprise, mais comme le dit l'adage, même si le changement est difficile, ne rien faire est encore plus difficile. Le changement nécessite bien sûr une stratégie bien planifiée, avec de nombreuses vérifications diligentes pour démontrer que la décision d'entrer sur un nouveau marché ou une nouvelle région, ou bien d'appliquer un nouveau modèle d'entreprise, est la bonne. Mais le défi du changement réside en grande partie dans les soft skills, la capacité à diriger, à persuader et à créer un consensus. La confiance est à la base de tous ces aspects.

Les dirigeants doivent convaincre les collaborateurs, les partenaires et les clients. L'IA replace la confiance sur le devant de la scène, car elle repose sur la collecte de vastes ensembles de données. Il n'a donc jamais été aussi important d'indiquer clairement quelles données sont collectées, comment elles sont obtenues et comment elles seront utilisées,

tout en faisant preuve de transparence quant aux facteurs de risque et à l'incertitude. Pour que l'IA ne soit pas source d'anxiété, nous devons dès à présent mettre en œuvre des politiques de protection et nous assurer que tout le monde y a accès et les comprend.

Quel est notre niveau de confiance dans l'IA aujourd'hui ? Faible, ce qui n'est pas surprenant face aux problèmes de l'IA générative comme les hallucinations (l'IA génère une réponse fausse qui est présentée comme un fait) ou les LLM qui reprennent des données de sources inconnues sur le Web et qui ne respectent pas toujours les droits d'auteur. Une nouvelle étude menée par FT Longitude pour Workday montre qu'il existe un fossé évident entre les dirigeants et les collaborateurs :

- **Attention au fossé :** 70 % des dirigeants accueillent favorablement l'IA et 65 % sont convaincus que leur entreprise la déploiera de manière fiable, contre 46 % et 51 % des collaborateurs, respectivement.
- **Diriger sans imposer :** quatre collaborateurs sur cinq déclarent ne pas avoir observé d'interactions collaboratives avec leur employeur au sujet de l'IA et n'avoir reçu aucune directive quant à son utilisation.
- **Éduquer et s'engager :** un collaborateur sur quatre n'est pas convaincu que son entreprise placera ses intérêts avant ceux de l'organisation. En outre, 69 % des dirigeants prévoient que l'IA réduira le travail manuel dans une large mesure, contre seulement 38 % des collaborateurs.

Cette étude vient confirmer les preuves existantes de l'importance de la confiance dans l'IA. Un rapport rédigé en 2023 par KPMG en collaboration avec l'université australienne de Queensland sur la base de 17 000 participants du monde entier a révélé des réactions extrêmement négatives, 61 % des personnes interrogées se déclarant indécises ou méfiantes à l'égard de l'IA.

Toutefois, en y regardant de plus près, les données sont plus nuancées avec, par exemple, beaucoup plus de réticence à faire confiance à l'IA dans les RH que dans le domaine du diagnostic médical. Il convient également de noter que les préjugés à l'égard de l'IA ne peuvent pas être attribués à la simple technophobie, 85 % des personnes interrogées affirmant que l'IA devrait apporter toute une série d'avantages.

Nous savons également que l'IA est l'un des phénomènes les plus importants et les plus rapides de l'histoire de la technologie, dont il est difficile de prévoir les prochaines évolutions quant à son fonctionnement, son application et son contrôle. Par conséquent, si votre entreprise mise sur l'IA pour apporter des changements significatifs, elle doit s'intéresser aux préoccupations de ses collaborateurs et partenaires, et trouver des solutions pour les atténuer.

Comme pour tout changement technologique majeur, nous savons que le chemin est semé d'embûches. Pensez au Cloud, au SaaS, à la blockchain ou au e-commerce : les obstacles à surmonter sont nombreux avant de se sentir à l'aise. Beaucoup d'entre nous ont l'impression de vivre dans la jungle, loin de ce que Gartner appelle le « Plateau de productivité ». Alors, comment l'atteindre ?

Établir la confiance de manière progressive

Voici quelques étapes pratiques identifiées lors de nos réflexions.

Utiliser une plateforme technologique de confiance

Nous serons peu nombreux à développer nos propres modèles LLM ou à ressentir le besoin de créer des applications centrales sur mesure en dehors de celles offrant un avantage concurrentiel direct. Nous devons donc sélectionner des fournisseurs et autres partenaires ayant de solides antécédents en matière de gestion des données et de mesures strictes de protection de l'IA.

70 % des dirigeants accueillent favorablement l'IA et 65 % sont convaincus que leur entreprise la déploiera de manière fiable.

Demandez à vos fournisseurs quelles pratiques concrètes ils appliquent en matière de gouvernance et de sécurité de l'IA. Demandez les noms de clients qui figurent parmi vos homologues. Recherchez des preuves de l'existence d'architectures qui évitent les biais grâce à des techniques telles que le « dynamic grounding » permettant de ne capturer que les informations les plus fiables et les plus récentes des LLM. Recherchez des contrôles d'accès et de récupération forts, ainsi que des capacités de masquage des données pour protéger les sources. Insistez sur des politiques de conservation strictes et sur la possibilité d'identifier et de bloquer les contenus toxiques. En outre, recherchez des fournisseurs qui participent activement à l'élaboration de normes et à la mise en place de mesures de protection pour l'IA.

Faire la distinction entre automatisation et augmentation

L'une des principales craintes suscitées par l'IA est une disruption massive des postes de bureau, certains emplois humains étant désormais considérés comme inutiles car pouvant être mieux réalisés par des machines. Les dirigeants doivent impérativement expliquer que l'IA vise à améliorer et à remplacer les tâches manuelles fastidieuses par l'intelligence des machines, libérant ainsi les hommes pour faire ce qu'ils font le mieux : faire preuve d'empathie et de créativité, collaborer et résoudre les problèmes.

La transparence étant le meilleur remède, il faut impliquer les collaborateurs et leur donner la parole. Accenture est un exemple d'entreprise qui a joué cartes sur table et a clairement indiqué qu'elle ne prévoyait pas de suppressions d'emplois, mais qu'elle s'attendait à des hausses massives de la productivité grâce à l'IA. Ce type de message clair contribuera grandement à rassurer le personnel susceptible de se sentir vulnérable ou exposé. Et si votre entreprise n'est pas dans cette optique et considère cette opportunité uniquement comme un moyen de procéder à des suppressions massives d'emplois et à des réductions de coûts, il est peut-être temps d'envisager vos autres options d'emploi.

Montrer l'exemple

L'homme politique qui affirme qu'il n'y aura pas d'augmentation d'impôts et qui les augmente quand même perd immédiatement la confiance de ses concitoyens. L'entreprise qui encourage un comportement éthique, puis exploite ses collaborateurs ou travaille avec des partenaires douteux, épuise son capital confiance. Les actes étant plus parlants que les mots, les promesses en matière d'IA doivent donc être suivies d'effets.

L'IA est une opportunité pour les DSI

Dans son livre *The Open Organization*, l'ancien CEO de Red Hat, Jim Whitehurst, fait l'éloge de la notion de démocratisation de la prise de décision dans toute l'entreprise, voire en dehors. D'après lui, les dirigeants doivent indiquer clairement lorsqu'ils ne savent pas quelque chose plutôt que de prétendre être omniscients.

La plupart des PDG modernes doivent être conscients des implications de l'IA pour leur entreprise, mais ils auront besoin de toute urgence de l'aide des DSI et d'autres spécialistes pour comprendre les complexités techniques, juridiques et éthiques. En instaurant la confiance et en se préparant dès maintenant à la probabilité d'une disruption massive provoquée par la technologie, les dirigeants avisés seront en mesure de surfer sur ce qui promet d'être l'une des grandes vagues stratégiques de notre époque.

Comme un DSI me l'a un jour dit, « la confiance est une rue à double sens, difficile à négocier. Personne ne sait exactement ce qui nous pousse à avoir confiance en l'autre. Mais nous savons qu'une fois que la confiance est perdue, c'est irréversible. Le message doit donc être transmis avec précaution. »

Tous les dirigeants doivent instaurer la confiance et comprendre pourquoi elle est préférable à des mesures de fidélisation rudimentaires qui donnent le sentiment d'être enfermé dans une « prison dorée ».

Points de vue d'experts sur l'avenir de l'IA dans les entreprises et la société

Par **Anja Fordon**,
rédactrice EMEA

Découvrez l'avis d'experts sur l'avenir de l'IA réunis lors de Workday Rising EMEA l'année dernière. Profitez des insights du docteur Tomas Chamorro-Premuzic et de bien d'autres.

Alors que l'IA et le Machine Learning (ML) font de plus en plus partie de notre vie quotidienne, il est plus que jamais essentiel d'en comprendre les implications. Lors de Workday Rising EMEA, des experts de différents domaines se sont réunis pour discuter du potentiel de transformation de l'IA et de la façon de combler le déficit de confiance en la matière. Découvrez leur point de vue.

Comprendre l'IA : faire la distinction entre engouement médiatique et réalité

« L'IA est une technologie incontournable de notre époque », a déclaré le docteur Tomas Chamorro-Premuzic, soulignant son caractère permanent et son impact. Cependant, il est nécessaire d'aller au-delà des opinions extrêmes des médias grand public pour nuancer la compréhension des capacités de l'IA et de ses limites. Cet éclairage équilibré est essentiel pour permettre aux collaborateurs et aux entreprises d'exploiter efficacement l'IA. Voici quelques-uns des points forts de la vidéo :

L'IA sur le marché du travail. Amplification et atténuation : Kathy Pham, Vice President AI & ML chez Workday, revient sur le contexte historique de la gestion du travail et de la Finance, notamment sur l'importance de comprendre ces processus dans le monde analogique avant d'intégrer l'IA. « La vitesse de la technologie et sa capacité à amplifier notre travail sont élevées », a-t-elle noté, suggérant que l'IA et le ML peuvent à la fois améliorer et remettre en question les pratiques traditionnelles dans l'entreprise.

« L'IA est une technologie incontournable de notre époque.

Docteur Tomas Chamorro-Premuzic,
Auteur et professeur de psychologie d'entreprise

Le reskilling à l'ère de l'IA : Le rôle des responsables Finance et RH dans la transition des collaborateurs de tâches de routine vers des activités essentielles est crucial, selon le docteur Tomas Chamorro-Premuzic. Cependant, ce changement n'est pas automatique. Il nécessite une gestion active et des mesures incitatives. L'upskilling est essentiel pour tirer parti de la prochaine évolution de l'IA.

Le déficit de confiance et l'interaction homme-machine : Filip Gilbert, Global Workday GTM & HR Technology Lead chez Accenture, a identifié un déficit de confiance envers l'IA quant à l'impact personnel et à l'employabilité. Instaurer la confiance implique de démontrer un investissement continu dans les collaborateurs et de rendre le rôle de l'IA dans l'amélioration des activités compréhensible et prévisible. « C'est l'interaction homme-machine [...] qui renforcera cette confiance », a-t-il affirmé. Fait intéressant, le docteur Tomas Chamorro-Premuzic a souligné que la méfiance à l'égard de l'IA est souvent le reflet d'une méfiance existante envers l'entreprise. La disparité dans la perception de l'IA entre les collaborateurs et les dirigeants indique un manque d'alignement des objectifs stratégiques de l'entreprise, problème qui nécessite l'intervention des dirigeants. Selon une nouvelle étude de Workday, un déficit de confiance en matière d'IA existe à tous les niveaux hiérarchiques et de façon plus prononcée chez les collaborateurs. Vous pouvez lire l'intégralité du rapport pour savoir comment combler ce déficit.

Réglementation, politiques et mise en œuvre de l'IA : Kathy Pham et Chandler Morse, Vice President Corporate Affairs chez Workday, sont revenus sur les opportunités pour les entreprises de collaborer avec les gouvernements sur la réglementation et les politiques en matière d'IA. Une telle collaboration peut améliorer les expériences utilisateur et les produits. Chandler Morse a également mentionné l'importance d'une mise en œuvre responsable et transparente de l'IA, soulignant le consensus parmi les leaders du secteur sur les meilleures pratiques en matière d'atténuation des biais, de confidentialité et d'explicabilité.

Ces insights des leaders du secteur fournissent une roadmap essentielle pour gérer les complexités de l'IA au travail et dans la société. En comblant le déficit de confiance, en favorisant une utilisation transparente et éthique de l'IA et en donnant la priorité au développement des compétences, nous pouvons exploiter le pouvoir de transformation de l'IA de manière responsable et efficace.

« La vitesse de la technologie et sa capacité à amplifier notre travail sont élevées.

Kathy Pham, Vice President AI & ML chez Workday

Trois conseils pour aider les DSI à s'adapter à l'évolution des réglementations de l'IA

L'arrivée de l'IA dans l'entreprise est de train de révolutionner notre façon de travailler, et nous pouvons nous attendre à une série de nouvelles réglementations pour encadrer son utilisation responsable. Mais comment les DSI peuvent-ils se préparer et répondre à ces nouvelles réglementations ? Voici trois conseils pour vous y aider.

Par **Steve Dunne**,
Rédacteur EMEA

Alors que les dirigeants mondiaux commencent à façonner les politiques en matière d'IA, les DSI doivent prêter une attention toute particulière à la transparence, à la confidentialité des données et à la responsabilité des fournisseurs.

L'IA évolue à une vitesse vertigineuse, mais comme souvent lorsqu'il s'agit de technologies, les réponses politiques ont du mal à suivre le rythme.

Les prochaines années promettent toutefois d'être importantes en matière de réglementation de l'IA, alors que les dirigeants mondiaux élaborent des politiques visant à régir les applications d'IA de nouvelle génération, y compris les grands modèles de langage (LLM) comme ChatGPT. Les décideurs politiques de l'Union européenne, par exemple, se sont mis d'accord sur les bases de la loi sur l'IA, un vaste ensemble de règles destinées à encadrer l'utilisation de l'IA pour en exploiter le potentiel tout en atténuant ses risques.

La forme exacte de cette réglementation de l'IA va continuer d'évoluer et nécessitera probablement de constantes mises à jour. Après tout, ChatGPT n'en est encore qu'à ses débuts. Voici toutefois quelques-unes des questions qui méritent d'être examinées :

- Dans une économie mondialisée, comment les différents pays permettront-ils et limiteront-ils l'utilisation de l'IA ?
- Comment l'IA peut-elle exploiter les données tout en garantissant que les informations sensibles restent sécurisées et protégées ?
- Quelles pratiques peuvent le mieux atténuer les biais dans les applications et les résultats de l'IA ?
- Quelle documentation sera nécessaire pour prouver que l'IA a été développée de manière responsable ?

Alors que les agences gouvernementales et les ONG continuent de se débattre avec ces questions cruciales, les DSI se retrouvent sur la sellette.

Même si aller de l'avant dans un contexte d'incertitude réglementaire comporte des risques, retarder le développement et le déploiement d'applications d'IA pourrait entraîner des conséquences à long terme sur la rentabilité et la croissance.

Risques mis à part, 60 % des entreprises adoptent l'IA et le Machine Learning (ML) d'une manière ou d'une autre, selon le rapport *C-Suite Global AI Indicator* de Workday. L'étude a par ailleurs révélé que la responsabilité d'un déploiement réussi de l'IA au sein de l'entreprise incombera aux leaders IT. Pour garder une longueur d'avance, les DSI doivent identifier la manière dont l'entreprise peut tirer profit de l'IA, définir des cas d'usage clairs et introduire des politiques de gouvernance qui permettront une utilisation responsable de l'innovation en matière d'IA.

« Si vous voulez réguler l'IA, vous ne pouvez pas le faire en régulant la technologie, car celle-ci évolue. Il faut donc réguler les utilisateurs et tenir compte du contexte, estime Thomas Boué, Director General, Policy, à la Business Software Alliance (BSA). Dans les utilisations à haut risque de l'IA, l'idée n'est pas d'empêcher l'innovation, mais de mettre en place des garde-fous pour garantir que l'IA puisse être utilisée, développée et déployée au profit de la société. »

Voici trois conseils à l'attention des DSI pour guider leurs pratiques en matière d'IA à mesure que la technologie et les réglementations évoluent.

La transparence avant tout

Si aucun DSI ne souhaite investir dans l'innovation pour voir ensuite des changements réglementaires le freiner dans son élan, l'IA n'en demeure pas moins une opportunité trop prometteuse pour la laisser passer. Pour réaliser des progrès significatifs dans un marché imprévisible, les DSI doivent exiger – et permettre – la transparence au sein de l'entreprise et de l'écosystème.

Cela commence par communiquer clairement où et comment l'IA sera utilisée, ainsi que les objectifs de l'entreprise en la matière. Avec tant d'inconnues encadrant le débat sur l'IA, une transparence radicale permet de définir les attentes quant à ce que les applications seront capables de réaliser, d'atténuer les craintes des acteurs impliqués et de faire preuve de responsabilité.

Les DSI peuvent promouvoir la transparence en levant le voile pour les acteurs impliqués internes et externes, y compris les régulateurs. Décrire dans le détail les pratiques de traitement des données et les mesures de confidentialité peut aider les entreprises à prouver que les données ont été utilisées de manière éthique et transparente. Expliquer quels algorithmes qui ont été choisis et pourquoi peut également montrer comment les biais sont pris en compte et traités.

Même si le type exact de documentation qui sera exigé par les organismes de réglementation reste à déterminer, « il existe un très fort consensus sur la transparence, explique Chandler Morse, Vice President, Public Policy chez Workday. Par exemple, l'avis général est que si l'on utilise l'IA dans les RH, il doit y avoir une transparence totale sur ce qui se passe, comment cela se passe, quelles données sont collectées et quelles conclusions sont tirées. »

Lorsque les entreprises communiquent ouvertement sur l'IA, les collaborateurs sont également plus disposés à poser des questions sur comment et où utiliser les nouvelles applications.

Cela réduit le risque que les équipes utilisent l'IA de manière inappropriée et augmente la probabilité qu'elles innovent en toute confiance et de manière responsable.

L'explicabilité réduit l'exposition aux risques

Alors que des directives de conformité sont en cours d'élaboration, l'explicabilité devrait être la boussole du DSI. Dans le contexte de l'IA, l'explicabilité concerne spécifiquement la prise de décision. La transparence offre une visibilité sur la manière dont l'IA est développée et déployée, mais l'explicabilité se concentre sur la façon dont le système pense, et sur la logique qu'il utilise pour tirer des conclusions.

« Que les gouvernements exigent une préapprobation réglementaire ou une auto-évaluation de l'IA – l'Union européenne a opté pour l'auto-évaluation, plaçant ainsi la responsabilité sur les développeurs de logiciels et les fournisseurs d'IA – les DSI devront pouvoir communiquer facilement le fonctionnement interne de ces applications », juge Jens-Henrik Jeppesen, Senior Director, Public Policy chez Workday. Par exemple, les entreprises peuvent être invitées à prouver qu'aucun matériel protégé par le droit d'auteur n'a été utilisé pour entraîner leur IA, même si un tiers a développé le modèle sur lequel elle est basée.

La gestion des collaborateurs en est un bon exemple. Lorsque l'IA est utilisée pour éclairer les décisions d'embauche, de promotion ou de licenciement, les DSI devront répondre à des questions sensibles sur la manière dont les technologies d'IA ont été entraînées, les biais traités et les données confidentielles protégées pendant la mise en œuvre. Il s'agit là d'un point crucial dans la mesure où certains pays envisagent une législation qui rend les

Les entreprises n'attendent pas que les gouvernements leur disent comment développer la technologie. Elles ont plutôt besoin de garde-fous pour garantir à leurs clients que ces produits et applications sont sûrs.

« Si vous voulez réguler l'IA, vous ne pouvez pas le faire en régulant la technologie, car celle-ci évolue. Il faut donc réguler les utilisateurs et tenir compte du contexte.

Thomas Boué, Director General, Policy, Business Software Alliance (BSA)

« L'avis général est que si l'on utilise l'IA dans les RH, il doit y avoir une transparence totale sur ce qui se passe, comment cela se passe, quelles données sont collectées et quelles conclusions sont tirées.

Chandler Morse, Vice President, Public Policy, Workday

entreprises utilisant des modèles d'IA à haut risque – tels que ceux destinés aux soins de santé ou à l'éducation – plus responsables de tout dommage résultant de cette utilisation.

Les modèles d'IA à usage général, appelés modèles de base, peuvent être ajustés pour accomplir tout un éventail de tâches. Les entreprises achètent souvent ces modèles généraux auprès de fournisseurs, mais une fois qu'une entreprise intègre un modèle de base dans ses produits ou ses opérations, ses dirigeants ont la responsabilité de garantir aux régulateurs que la technologie est conforme aux nouvelles règles. Cela signifie que les DSI doivent s'assurer qu'ils reçoivent une documentation complète comprenant des informations sur l'architecture des modèles, l'ingénierie des fonctionnalités, les procédures de test et les mesures de sécurité.

« Les entreprises doivent donc avoir de vrais échanges avec leurs fournisseurs pour s'assurer qu'ils maîtrisent parfaitement les réglementations émergentes et qu'ils disposent de programmes de gouvernance qui s'alignent sur ces exigences réglementaires émergentes », rappelle Jens-Henrik Jeppesen.

Les DSI doivent également savoir où les équipes internes utilisent le modèle de base, comment ce modèle a été intégré aux produits et opérations de l'entreprise et quelles données supplémentaires ont été utilisées pour affiner l'application. À mesure que l'adoption augmente, garantir l'explicabilité devient une tâche qui s'étend à toute l'entreprise. « L'IA n'est plus un outil standard qu'il suffit d'installer sur votre système pour qu'il fonctionne, avertit Thomas Boué. Il s'agit de quelque chose qui se négocie, se discute et qui change tout le temps. »

Des garanties pour encourager l'innovation

Les entreprises réclament rarement plus de réglementation, mais lorsqu'il s'agit d'IA, la plupart des acteurs du secteur s'accordent sur la nécessité de meilleures garanties.

Les entreprises n'attendent pas que les gouvernements leur disent comment développer la technologie. Elles ont plutôt besoin de garde-fous pour garantir à leurs clients que ces produits et applications sont sûrs. « La sûreté réglementaire s'accompagne d'un certain niveau de confiance », explique Chandler Morse.

Pour renforcer la confiance pendant l'élaboration des réglementations, les DSI doivent examiner ce que font les leaders de l'IA dans ce domaine. Les précurseurs qui déploient l'IA pour les RH se concentrent par exemple sur la protection des droits fondamentaux des collaborateurs individuels, des candidats et des postulants à chaque étape du processus.

Adopter une approche proactive prépare également les entreprises multinationales aux inévitables variations de la législation sur l'IA à travers le monde. Définir les termes clés et s'aligner sur les principes fondamentaux de l'IA responsable, notamment la transparence, l'explicabilité, l'atténuation de la discrimination et des biais, ainsi que la protection de la vie privée, peut aider les entreprises à aller plus loin plus rapidement, tout en permettant également la collaboration entre les juridictions.

« Il existe un objectif commun, à savoir disposer d'un environnement interopérable pour l'innovation et le déploiement de ces technologies, estime Jens-Henrik Jeppesen. La plupart des pays ont des objectifs globalement similaires : bénéficier de tous les avantages de cette technologie, tout en garantissant qu'elle est sûre, fiable et qu'elle peut être utilisée en toute confiance. »

Cinq façons pour les plateformes technologiques de protéger les données privées

Les données sont l'élément vital de nombreuses entreprises, mais non protégées, elles peuvent faire plus de mal que de bien. Alors que la confidentialité des données fait l'objet d'une attention accrue, voici les outils et les pratiques pour renforcer la confidentialité et la sécurité des données.

Par **Patrick Evenden**,
Rédacteur EMEA

Alors que les données privées deviennent plus importantes que jamais, elles sont aussi plus difficiles à protéger. Les pirates utilisent l'IA pour s'introduire plus rapidement et plus efficacement dans les systèmes informatiques, et les entreprises doivent renforcer leur sécurité pour ne pas devenir leur prochaine victime. Dans le même temps, les réglementations évoluent rapidement, plaçant la barre de la conformité toujours plus haut.

Dans ce contexte, les dirigeants d'entreprise déclarent que la sécurité et la confidentialité sont les principaux risques liés à l'utilisation de l'IA et du Machine Learning (ML) dans leur entreprise, selon le rapport *C-Suite Global AI Indicator* de Workday. Pour maîtriser ces risques tout en tirant parti de l'IA, les DSI ont besoin d'une technologie plus performante sur tous les fronts.

En plus de faciliter l'organisation et l'analyse des données, les plateformes technologiques peuvent aider les entreprises à garder une longueur d'avance sur les cybermenaces et les règles en matière de protection de la vie privée. Avec les bons outils Cloud, les équipes IT peuvent intégrer en amont la protection de la vie privée dans les systèmes, plutôt que de réagir après-coup face aux nouveaux risques et nouvelles réglementations.

Voici cinq façons dont les plateformes technologiques peuvent aider les entreprises à répondre aux nouveaux besoins en matière de protection de la vie privée en ces temps incertains.

1. Rendre la transparence automatique

La collecte de données sur les utilisateurs présente d'innombrables avantages, mais aussi de gros risques. Non seulement la plupart des juridictions appliquent des règles strictes quant à la manière dont les données privées peuvent être collectées et utilisées (règles appelées à se renforcer avec l'utilisation accrue de l'IA et du Machine Learning), mais elles exigent également des entreprises qu'elles décrivent clairement aux utilisateurs ce qu'elles prévoient de faire avec ces données.

« Ces dernières années, certaines entreprises ont été sanctionnées par des amendes de plusieurs millions de dollars pour n'avoir pas respecté les exigences en matière de transparence et de diffusion des informations », rappelle Patricia O'Gara, Senior Principal, Data & Privacy Engineering chez Workday.

Une transparence totale est nécessaire pour permettre aux utilisateurs finaux de décider en connaissance de cause du type d'autorisations qu'ils souhaitent accorder à une entreprise. Mais il peut être difficile de fournir les informations légales dont ils ont besoin d'une manière accessible. Avec la bonne plateforme technologique, les entreprises peuvent constamment communiquer les informations sur la protection de la vie privée : sur une page d'accueil, dans un pied de page ou dans un tableau de bord central consulté fréquemment par les utilisateurs. Quelle que soit la manière utilisée, des liens clairs vers les avis de confidentialité, qui peuvent être mis à jour si nécessaire, permettent aux utilisateurs d'accéder aux informations requises d'un simple clic.

Seulement 34 % des personnes interrogées dans le cadre d'une enquête mondiale sur la protection de la vie privée ont déclaré avoir procédé à un mappage de données et comprendre les pratiques de leur entreprise en matière de données.

2. Donner le contrôle aux utilisateurs

La plupart des lois sur la protection de la vie privée partent du principe que les individus doivent avoir le contrôle de leurs données. Malgré l'évolution continue des exigences, les entreprises proactives peuvent garder une longueur d'avance en laissant les utilisateurs décider quelles données peuvent être utilisées et à quelles fins.

Par exemple, une entreprise peut vouloir suivre des mesures sur les utilisateurs de son site Web à l'aide d'un logiciel d'analyse. Elle peut ainsi personnaliser le marketing, les messages axés sur la carrière ou les offres futures, à condition que les utilisateurs acceptent de partager ce type de données via des bannières de cookies.

Cependant, il ne s'agit là que d'une pièce du puzzle. Les utilisateurs doivent également pouvoir contrôler la manière dont leurs données sont stockées et traitées, ce qui exige des entreprises qu'elles les informent de l'envers du décor. Par exemple, si un collaborateur demande à avoir accès à ses données personnelles, les équipes IT doivent pouvoir créer rapidement un rapport indiquant quelles sont les informations suivies par l'entreprise, qui peut y accéder et comment elles sont exploitées pour éclairer la prise de décision. Toutefois, de nombreuses entreprises ont encore des progrès à faire : seulement 34 % des personnes interrogées dans le cadre d'une enquête mondiale sur la protection de la vie privée ont déclaré avoir procédé à un mappage de données et comprendre les pratiques de leur entreprise en matière de données.

Des guides d'administration et des fiches d'information peuvent aider les entreprises à communiquer clairement sur la manière dont les données personnelles sont utilisées par les modèles de ML, en donnant aux utilisateurs le contexte dont ils ont besoin pour accorder des autorisations de manière éclairée.

« Il s'agit en fait de savoir quelles sont les données utilisées en entrée, quel est le résultat du Machine Learning, comment nous évaluons les biais et comment notre propre modèle de Machine Learning est entraîné, explique Sabine Hagege, Director, HCM Product Strategy chez Workday. Les utilisateurs ont besoin de beaucoup d'informations pour comprendre comment les données sont traitées. »

3. Obtenir un consentement granulaire

Dans de nombreuses situations, les utilisateurs n'hésiteront pas à partager certaines informations personnelles à des fins spécifiques. Les entreprises doivent alors veiller à ce que les données soient utilisées de manière appropriée. Et si une entreprise compte des clients ou des collaborateurs dans plusieurs juridictions, elle doit s'assurer que les données ne sont pas partagées avec ou recueillies depuis des régions où les lois sur la protection de la vie privée sont différentes.

Comment les DSI peuvent-ils s'y retrouver ? D'abord, avec une configuration adéquate. Les plateformes technologiques qui offrent un cadre de localisation permettent aux équipes IT de déterminer quel type d'information peut être exploité pour différentes personnes en fonction de leur identité, de leur rôle et de leur localisation.

« L'idéal est de pouvoir configurer le système en fonction de l'objectif de la collecte de données. Est-elle effectuée dans le cadre de la diversité et de l'inclusion ou celui du recueil de statistiques et de mesures ?, explique Sabine Hagege. Ensuite, pour chaque pays, utilisez la réponse à la demande de consentement pour configurer vos autres processus et contrôler la manière dont ces données sont utilisées. »

Comment les DSI peuvent-ils s'y retrouver ? D'abord, avec une configuration adéquate.

Il s'agit en fait de savoir quelles sont les données utilisées en entrée, quel est le résultat du Machine Learning, comment nous évaluons les biais et comment notre propre modèle de Machine Learning est entraîné.

Sabine Hagege, Director, HCM Product Strategy, Workday

4. Purger les données inutiles

De nombreuses règles de protection de la vie privée exigent également la suppression des données personnelles qui ne sont plus nécessaires. Le consentement doit être donné pour un but et un délai précis, et les entreprises doivent ensuite effacer ou purger ces informations de manière définitive.

Pour respecter les attentes et les réglementations, chaque entreprise a besoin d'un plan de purge des données. Les DSI doivent travailler avec leurs équipes IT pour déterminer quelles données doivent être purgées et à quel moment, puis planifier des suppressions en masse à intervalles réguliers.

Mais cela ne suffit pas. Les entreprises doivent également pouvoir purger à volonté les données d'un individu, soit parce que son statut a changé, soit parce qu'il en fait la demande. Par exemple, un DSI peut vouloir que les données de chaque collaborateur licencié soient effacées immédiatement après son départ de l'entreprise. Un candidat à un emploi peut également demander la suppression de ses données s'il n'est pas embauché.

Les services IT doivent faciliter la suppression des données, sans jamais oublier que « la purge est définitive », selon Sabine Hagege : « Il est donc très important de mettre en place des contrôles et de s'assurer que toute personne autorisée à purger des données est parfaitement consciente que cette action est irréversible. »

5. Préserver la confidentialité des données privées

Obtenir le consentement pour collecter et utiliser des informations privées ne rend pas ces données moins privées. Les DSI doivent en être conscients lorsqu'ils déterminent qui peut consulter quelles données, et prendre les mesures nécessaires pour préserver la confidentialité des informations sensibles.

Certains types de données, comme les dates de naissance, les numéros d'identification nationale (comme le numéro de sécurité sociale) et les données médicales, ont une grande valeur sur le marché noir. Parce que ces types de données sont une cible privilégiée pour le vol ou l'exploitation, ils doivent être traités avec beaucoup de précautions à chaque étape.

Par exemple, lorsque les équipes IT mettent en œuvre de nouvelles fonctions ou fonctionnalités de plateforme, elles peuvent occulter les données privées pour empêcher les testeurs d'y avoir accès. Le processus d'occultation des données utilise de vraies données personnelles pour créer des jeux de données réalistes mais factices à l'intention des testeurs. Cela permet d'assurer le contrôle qualité cohérent et rigoureux nécessaire au déploiement de nouvelles technologies tout en limitant l'exposition.

Le masquage des données permet également aux entreprises de préserver la confidentialité des données privées. Par exemple, tandis qu'un responsable a besoin de connaître le salaire d'une personne, ce n'est pas le cas de tous les membres du service RH. La communication des données privées selon le principe strict du « besoin d'en connaître » peut protéger la vie privée et la sécurité des collaborateurs, tout en aidant les entreprises à respecter les diverses législations locales en matière de protection de la vie privée.

« Il s'agit d'une sécurité contextuelle, très utile dans les multinationales, indique Patricia O'Gara. C'est un modèle entièrement flexible qui permet un contrôle total sur qui a accès à quoi. »

Les utilisateurs doivent également pouvoir contrôler la manière dont leurs données sont stockées et traitées, ce qui exige des entreprises qu'elles les informent de l'envers du décor.

Renforcer la confiance et l'enthousiasme des collaborateurs grâce à l'IA responsable

L'IA, en particulier l'IA générative, n'en est qu'à ses débuts, ce qui suscite chez les collaborateurs des degrés divers d'anticipation, d'incertitude et de méfiance. Pour instaurer la confiance, les entreprises devront avoir des échanges honnêtes, mettre en place des politiques claires et faire de la formation une priorité.

Par **Emily Teesdale**, Senior Manager, KPMG

Mohammed Bari, Director, Powered HR, KPMG

L'IA générative promet d'ouvrir une nouvelle ère de productivité, et les entreprises qui prendront les bonnes décisions pourraient bien prendre une avance considérable sur leurs concurrents. Mais personne ne peut encore dire avec certitude en quoi consistera cette promesse.

Cette technologie émergente, qui utilise des algorithmes avancés de Machine Learning (ML) pour générer des contenus entièrement nouveaux (textes, images, vidéos, présentations, etc.) est encore en phase d'expérimentation dans le monde de l'entreprise. Pourtant, les dirigeants comprennent l'urgence de la situation : selon une étude internationale de Workday, 80 % des décideurs reconnaissent que l'IA est nécessaire pour que leur entreprise reste compétitive, conscients que, s'ils attendent que l'IA générative fasse ses preuves pour prendre le train en marche, leur entreprise pourrait rapidement se retrouver à la traîne.

Pour garder une longueur d'avance, les entreprises expérimentent sur de nombreux fronts. De l'automatisation de tâches complexes au brainstorming de solutions créatives, elles cherchent de nouveaux moyens d'améliorer l'efficacité et d'accélérer l'innovation. Les possibilités sont passionnantes, mais on ne sait pas encore très bien ce que cette technologie signifiera pour les collaborateurs.

Dans l'ensemble, les DSI s'attendent à ce que l'augmentation de la productivité, le renforcement de la collaboration et l'augmentation des revenus et des bénéfices soient les principaux avantages découlant de l'intégration de l'IA et du ML au sein de la fonction IT, selon un rapport de Workday. Toutefois, selon une enquête de Forrester Consulting, seul un tiers des collaborateurs déclare avoir une bonne compréhension de l'IA et de la manière dont elle peut être utilisée au travail.

Par ailleurs, l'adoption de l'IA générative s'accompagne de plusieurs défis fondamentaux pour les entreprises. Formation éthique, utilisation responsable, gouvernance solide et conformité réglementaire ne sont que quelques-uns des facteurs essentiels que les DSI doivent prendre en compte.

Sans une gouvernance appropriée, l'IA peut créer plus de problèmes qu'elle n'en résout.

« ChatGPT et d'autres outils d'IA générative répondront à vos questions avec beaucoup d'assurance, mais en se basant sur les données auxquelles ils ont accès. Or, ces données ne sont pas toujours exactes, rappelle Emily Teesdale, Senior Manager chez KPMG. Beaucoup d'entreprises se lancent donc dans l'élaboration de politiques et de procédures pour gérer ces risques inhérents. »

La manière dont les entreprises exploitent, entraînent et affinent les outils d'IA générative pourrait également avoir une incidence majeure sur la confiance des clients et des collaborateurs. Pour favoriser l'adhésion, les leaders IT doivent démontrer que l'IA peut être déployée de manière responsable, c'est-à-dire en protégeant la vie privée, en préservant les emplois et en générant des contenus exacts.

De leur côté, les collaborateurs veulent approfondir la question de l'IA. Ils sont environ trois sur quatre à espérer que leur entreprise explore davantage les possibilités de mise en œuvre. Mais les entreprises doivent trouver un juste équilibre entre innovation et éthique pour susciter l'enthousiasme à l'égard des nouvelles méthodes de travail. Dans le cas contraire, la résistance interne au changement pourrait entraver la réalisation de progrès significatifs.

Voici comment les DSI peuvent adopter et mettre en œuvre des solutions d'IA générative qui permettront à la fois d'améliorer les résultats et de donner aux collaborateurs les moyens de participer à un changement responsable.

Les collaborateurs veulent approfondir la question de l'IA. Ils sont environ trois sur quatre à espérer que leur entreprise explore davantage les possibilités de mise en œuvre.

Élaborer (et communiquer) une stratégie claire en matière d'IA

Bien que l'IA générative ait quelque chose de magique, la déployer avec succès ne se fait pas du jour au lendemain. Pour aller plus vite avec cette technologie, il faut avoir une vision claire de ce que l'entreprise veut réaliser, qu'il s'agisse de stimuler la productivité, d'accroître la satisfaction client ou d'améliorer l'expérience collaborateur. À partir de là, les équipes peuvent commencer à réfléchir à différents moyens d'atteindre ces objectifs.

Toutefois, les résultats dépendront de la qualité et de la quantité des données auxquelles les modèles d'IA ont accès. Bien que certaines solutions prêtes à l'emploi soient pré-entraînées sur des jeux de données pertinents, la plupart des modèles doivent être affinés à l'aide de données propriétaires pour fournir les résultats les plus significatifs. Les DSI doivent donc s'efforcer de relier les données internes de manière responsable.

Les DSI doivent également veiller à ce que la stratégie d'IA de l'entreprise ne perde pas de vue l'évolutivité, en réfléchissant à la manière dont les nouvelles solutions s'intégreront aux processus existants. Il s'agit d'améliorer les résultats tout en restant agile, en adoptant une technologie capable de s'adapter à l'évolution de l'entreprise et des applications d'IA.

Si une planification stratégique proactive est essentielle pour rendre les investissements dans l'IA générative aussi efficaces que possible, cela ne signifie pas que les DSI ont besoin d'un plan entièrement élaboré pour commencer, rassure Mohammed Bari, Director, Powered HR, chez KPMG.

Il ajoute : « Vous pouvez préparer une stratégie tout en analysant vos cas d'usage. Mais n'attendez pas. Allez-y, lancez-vous. Commencez à réfléchir, à faire du brainstorming et à expérimenter. »

Commencer par des cas d'usage spécifiques ciblant les points de friction

Votre stratégie d'IA générative indique aux équipes la direction qu'elles doivent prendre. Des cas d'usage spécifiques leur indiquent la voie à suivre, et cette orientation supplémentaire peut faire toute la différence.

« Il s'avère que l'IA est davantage axée sur les cas d'usage, explique Mohammed Bari. Si je rencontre des difficultés dans le recrutement et le redéploiement des talents, je dois me demander de quelle manière l'IA peut m'aider à résoudre ces problèmes. »

Prenons l'exemple d'une entreprise qui reçoit des milliers de CV chaque jour. S'il est impossible pour une seule personne de tous les examiner, l'IA générative peut aider à faire émerger les meilleurs candidats. En se concentrant sur les compétences (celles dont l'entreprise dispose, celles dont elle a besoin et celles que les différents candidats peuvent lui apporter), l'IA générative peut rapidement trouver le meilleur profil. Grâce à une marketplace des compétences interne, les entreprises peuvent également trouver rapidement les parfaits candidats qu'ils ont déjà à disposition.

Bien que les détails de chaque cas d'usage varient, se concentrer sur les principaux points de friction peut aider les entreprises à obtenir des gains rapides, tout en aidant les équipes à mieux comprendre comment l'IA générative fonctionne réellement. Lorsque les collaborateurs commenceront à appliquer cette technologie dans leurs tâches quotidiennes, ils identifieront des utilisations potentielles qui faciliteront leur travail. L'investissement personnel des collaborateurs dans les déploiements de l'IA s'accompagnera de gains de productivité plus importants.

Seuls 16 % des dirigeants estiment que l'adhésion des collaborateurs est essentielle à la réussite de l'IA.

« ChatGPT et d'autres outils d'IA générative répondront à vos questions avec beaucoup d'assurance, mais en se basant sur les données auxquelles ils ont accès. Or, ces données ne sont pas toujours exactes.

Emily Teesdale, Senior Manager, KPMG

Donner la priorité à l'éthique et à la gouvernance dès le départ

Les modèles d'IA sont entraînés à partir d'énormes jeux de données, mais cela ne signifie pas que ces données sont toujours exactes. Il existe donc un risque de biais, reproduisant les préjugés inconscients des humains chargés de l'entraîner, ou un risque d'erreurs pures et simples. Il y a aussi le risque que les données d'entraînement aient été manipulées par des acteurs malveillants, ce type de cyberattaque devenant de plus en plus lucratif et donc courant.

Dans ce contexte, les DSI doivent élaborer un plan complet de gestion des risques tenant compte de ces menaces afin de développer et d'acquérir des solutions d'IA dans lesquelles ils peuvent avoir confiance. En définissant des lignes directrices pour utiliser l'IA de manière responsable, respecter la confidentialité des données et faire preuve de transparence, vous montrez à vos collaborateurs que vous vous préoccupez des questions éthiques, et vous les responsabilisez. Si les DSI doivent montrer l'exemple, une IA digne de confiance nécessite l'engagement de tous les acteurs impliqués.

Pour susciter l'engagement des collaborateurs, proposez des formations régulières sur la politique éthique de l'entreprise, les réglementations pertinentes et la manière d'identifier et de traiter les questions éthiques. Encouragez une communication ouverte en indiquant clairement aux collaborateurs comment faire part de leurs préoccupations et en établissant des politiques de signalement qui les protègent des représailles. Luttez contre les biais avant qu'ils ne deviennent un problème en augmentant la diversité dans les équipes qui développent et utilisent de nouvelles applications d'IA. En prenant ces mesures dès le début, l'entreprise montrera à ses collaborateurs qu'elle prend au sérieux son engagement en faveur de l'IA responsable.

Pour susciter l'engagement des collaborateurs, proposez des formations régulières sur la politique éthique de l'entreprise, les réglementations pertinentes et la manière d'identifier et de traiter les questions éthiques.

Tenir compte du facteur humain

L'IA générative pourrait complètement transformer le paysage économique, et les collaborateurs ne sont pas tout à fait sûrs de ce que cela impliquera pour eux. Par exemple, les gains de productivité se traduiront-ils par des licenciements ? Ou bien leurs fonctions évolueront-elles d'une manière qui dépasse leurs compétences ?

Ces inquiétudes sont réalistes et les DSI doivent les prendre au sérieux. Si les équipes ne sont pas disposées à trouver de nouvelles façons de travailler avec l'IA générative, l'innovation sera bloquée. Pourtant, seuls 16 % des dirigeants estiment que l'adhésion des collaborateurs est essentielle à la réussite de l'IA.

Pour que les collaborateurs participent activement à l'innovation en matière d'IA, prenez le temps de leur montrer où les humains apportent le plus de valeur ajoutée. Mettez en évidence les tâches stratégiques, créatives et logiques qui requièrent un esprit humain perspicace. Ensuite, aidez-les à explorer comment l'IA générative peut valoriser leur propre rôle en automatisant les tâches banales que personne ne veut faire.

Tout le monde ne sera pas ouvert au changement, il faut donc identifier ceux qui sont prêts à s'adapter et investir en eux en tant que leaders de la conduite du changement. Contrairement aux compétences, l'attitude ne s'enseigne pas. Dans un climat incertain, cultiver l'enthousiasme, la curiosité et l'empathie sera la clé de la réussite future, estime Mohammed Bari.

« Les choses qui nous rendent humains, qui font de nous de bonnes personnes et de bons collègues, sont celles qui nous permettront de nous démarquer », explique-t-il.

À propos de KPMG UK

KPMG LLP, une société britannique à responsabilité limitée, possède 20 bureaux au Royaume-Uni, ce qui représente environ 18 000 partenaires et collaborateurs. Elle est présente dans 143 pays et territoires et compte plus de 273 000 partenaires et collaborateurs travaillant dans des cabinets membres à travers le monde.

Comment les entreprises peuvent prospérer grâce à une IA de confiance

Les applications exactes de l'IA ne sont pas toutes connues, mais les entreprises devraient prendre en compte la protection de la vie privée, le jugement humain et la simplification des systèmes pour guider son utilisation avec succès.

Par **Anja Fordon**, rédactrice EMEA

De la rédaction de contenu marketing à l'élaboration de prévisions financières plus rapides et plus précises, en passant par la rationalisation des chaînes d'approvisionnement, les dirigeants sont conscients des opportunités incroyables qu'offre la mise en œuvre de l'IA dans l'entreprise.

Et aucun ne veut rater le train en marche : près des trois quarts d'entre eux se sentent contraints de renforcer l'adoption de l'IA, selon le rapport Workday de 2023 sur le QI de l'IA. Ce que l'on ne sait pas encore, c'est où et comment l'IA apportera les gains les plus importants.

« Ce que nous aurions fait il y a six mois n'est pas ce que nous faisons aujourd'hui. Et nous ne savons pas aujourd'hui ce que nous ferons dans six mois », explique Shane Luke, Vice President, AI and Machine Learning (ML) chez Workday.

Pour atteindre le potentiel incroyable annoncé, les DSI doivent aider leur entreprise à traverser un champ miné de problèmes encore méconnus liés à la vie privée, à la sécurité, aux biais et à l'éthique. Or, les politiques, les règles et les meilleures pratiques qui devraient normalement les guider sont encore en cours d'élaboration. Face à autant d'incertitudes, il n'est pas surprenant que près de la moitié (49 %) des PDG estiment que leur entreprise n'est pas prête à adopter l'IA et le ML, selon le rapport *C-Suite Global AI Indicator* de Workday.

« Si les utilisateurs ne font pas confiance à la technologie, ils ne l'utiliseront pas, avertit Tom Girdler, Principal, Product Marketing chez Workday. En revanche, si nous nous appuyons sur un cadre solide pour mettre au point cette technologie, cela créera une dynamique très intéressante où la confiance et l'IA pourront vraiment se développer en synergie. »

En renforçant la confiance dans l'IA, les DSI peuvent en accélérer l'adoption et commencer à fournir la valeur exponentielle attendue par les dirigeants d'entreprise. Comment y parvenir ? Il faut d'abord adhérer aux trois principes d'une IA digne de confiance et permettre aux équipes d'expérimenter de manière responsable cette technologie transformatrice.

> « Ce que nous aurions fait il y a six mois n'est pas ce que nous faisons aujourd'hui. Et nous ne savons pas aujourd'hui ce que nous ferons dans six mois.
>
> **Shane Luke,** Vice President, AI and Machine Learning (ML), Workday

1. Évaluer les risques en matière de protection de la vie privée et planifier la mise en conformité

Toutes les applications de l'IA ne présentent pas le même niveau de risque. Pour faire face à l'évolution des questions de confidentialité et de conformité, les équipes IT doivent comprendre les problèmes particuliers que pose chaque cas d'usage et aider l'entreprise à hiérarchiser les projets en conséquence.

Certains risques doivent être jugés inacceptables dès le départ, comme la présence de biais ou de discriminations dans les modèles d'IA qui pourraient conduire à des résultats injustes ou discriminatoires concernant l'origine ethnique, le sexe ou d'autres caractéristiques protégées. Les failles de sécurité, la collecte non autorisée de données et les prédictions peu fiables sont d'autres exemples de risques inacceptables qui devraient stopper net un projet d'IA.

D'autres risques peuvent être gérés, mais nécessitent une surveillance étroite. Par exemple, de nombreux modèles d'IA apprennent au fur et à mesure qu'ils sont utilisés, ce qui signifie que de nouvelles interactions peuvent introduire de nouveaux types de biais. Les équipes IT doivent définir des lignes directrices à l'intention des utilisateurs qui fournissent de nouvelles données d'entrée, et surveiller les données de sortie en évolution pour s'assurer qu'elles restent justes et exactes.

Les DSI doivent également garder un œil sur la conformité. Alors que la plupart des lois sur la protection de la vie privée ne sont pas encore à jour des dernières avancées en matière d'IA, les leaders IT doivent se préparer à ce qui est à venir. Les réglementations varieront certainement d'un pays à l'autre, mais il existe un large consensus sur le fait que quelques facteurs clés sont essentiels au développement et au déploiement d'une IA digne de confiance.

« Il est question de transparence, de documentation technique, de tenue de registres, de surveillance humaine, d'exactitude, de robustesse et de cybersécurité, explique Jens-Henrik Jeppesen, Senior Director, Public Policy chez Workday. L'idée est que des normes techniques seront élaborées pour répondre à chacune de ces exigences réglementaires et que les entreprises se certifieront selon ces normes. »

2. Maintenir les humains à la barre

Les auteurs de science-fiction adorent imaginer des futurs dystopiques régis par des IA sensibles. Bien sûr, les technologues savent que l'IA ne peut pas penser et qu'elle ne peut que tirer des conclusions sur la base de ses données d'entraînement. Mais cela aussi peut s'avérer dangereux.

Lorsque des machines dénuées de toute réflexion prennent des décisions purement basées sur des données, elles ignorent souvent des facteurs contextuels cruciaux. Par exemple, un modèle financier piloté par l'IA qui s'appuie sur des données historiques pour faire des projections peut ne pas tenir compte des conditions géopolitiques actuelles ou des changements récents dans le sentiment du marché, qui pourraient influencer de manière significative les résultats de l'entreprise.

Pour que l'IA puisse éclairer efficacement les décisions, les humains doivent rester impliqués à chaque étape du processus. De l'entraînement à l'adoption, en passant par les tests et la mise en œuvre, les entreprises doivent utiliser l'IA pour amplifier le potentiel humain, et non l'inverse.

« La vraie question est de savoir comment mettre cela en pratique », s'interroge Kelly Trindel, Chief Responsible AI Officer chez Workday.

« Cela nécessite une collaboration interdisciplinaire et une ouverture d'esprit », explique-t-elle. Dans les premiers temps, les DSI doivent mettre en place les équipes et les structures organisationnelles nécessaires pour élaborer les lignes directrices qui favoriseront l'équité, l'exactitude, la fiabilité et la robustesse au fur et à mesure que l'entreprise mettra en œuvre de nouvelles applications.

77 % des dirigeants craignent qu'au moins une partie de leurs données ne soient ni suffisamment à jour ni suffisamment fiables pour être utilisées avec l'IA et le ML.

« Ceux qui savent réellement comment ces choses fonctionnent doivent être impliqués dans la mise en place de la gouvernance de l'IA, souligne Kelly Trindel. Selon nous, le fait d'avoir des lignes hiérarchiques distinctes pour ceux qui développent la gouvernance des systèmes d'IA et ceux qui sont les développeurs de première ligne des systèmes d'IA est une bonne pratique à développer. »

3. Concevoir des systèmes plus simples pour atténuer les biais

Il est impossible d'éviter complètement les biais dans l'IA. Les êtres humains ont chacun leurs opinions et entraînent l'IA sur la base de ce qu'ils croient être vrai. Cependant, le fait de travailler de manière proactive à l'atténuation de ces préjugés dès le départ peut contribuer grandement à la mise en place de systèmes d'IA plus éthiques et plus équitables.

« La conception du système est de loin la partie la plus importante, estime Shane Luke. Il est possible de concevoir le système de manière à ce qu'il soit très peu probable qu'il produise quelque chose que l'on ne souhaite pas. Il s'agit là du véritable point de départ. »

Les données d'entraînement déterminant ce que produit l'IA, les DSI doivent s'assurer que toutes les applications sont construites à partir de données fiables qui ont été examinées et validées par diverses équipes humaines. Bien qu'il soit important de tester les données de sortie pour atténuer les biais qui se glissent dans le modèle, cela doit être le filet de sécurité de l'entreprise et non sa première ligne de défense, souligne Shane Luke : « Il ne s'agit pas d'essayer de vérifier ou de contrôler les données de sortie. C'est beaucoup plus difficile à faire et ce n'est jamais un processus définitif. »

Par exemple, les grands modèles de langage (LLM) tels que ChatGPT sont entraînés sur de vastes jeux de données généraux qui leur permettent de fournir des réponses longues dans un langage naturel convaincant. Mais ces jeux de données comprennent souvent un contenu de mauvaise qualité, comme des informations erronées trouvées en ligne. Un pourcentage important des dirigeants (77 %) s'inquiètent du fait qu'au moins une partie de leurs données ne soient ni suffisamment à jour ni suffisamment fiables pour être utilisées avec l'IA et le ML. Comme alternative, les DSI et ceux qui conçoivent les systèmes doivent envisager de créer des applications de portée plus réduite, entraînées pour accomplir des tâches très spécifiques.

« Comme ces applications sont plus limitées, elles fascinent moins, indique Shane Luke. Mais elles sont très efficaces pour les tâches qu'elles sont censées accomplir, tout en étant moins susceptibles de faire quelque chose que vous ne souhaitez pas. »

« Il est question de transparence, de documentation technique, de tenue de registres, de surveillance humaine, d'exactitude, de robustesse et de cybersécurité.

Jens-Henrik Jeppesen, Senior Director, Public Policy, Workday

Instaurer la confiance à l'heure de l'insécurité des données grâce à une stratégie proactive

Maîtriser la confidentialité des données nécessite de s'engager à cartographier continuellement les risques. Pour atteindre cet objectif, la première étape consiste à adopter les meilleures pratiques et les outils automatisés qui vont effectuer le gros du travail.

Par **Steve Dunne**,
Rédacteur EMEA

Les données sont l'élément vital de l'économie digitale d'aujourd'hui, mais cela ne vaut que si elles sont fiables. Si elles alimentent l'innovation et l'agilité, elles sont aussi au cœur de la multiplication des menaces pour la sécurité et du renforcement des exigences réglementaires. La capacité à trouver le bon équilibre entre la protection des données et l'excellence opérationnelle est de plus en plus liée à la capacité à inspirer la confiance des clients, des collaborateurs et des investisseurs.

Selon un rapport IDC de septembre 2023, de nombreuses entreprises ont connu une hausse des cyberattaques d'une année sur l'autre, y compris 54 % des entreprises européennes. C'est l'une des raisons pour lesquelles la sécurité des données figure désormais en tête des priorités des dirigeants de tout le continent. Concrètement, 45 % des chefs d'entreprise interrogés en Europe ont déclaré qu'ils donneraient la priorité aux dépenses liées à la sécurité des données, à l'atténuation des risques et à la conformité pour soutenir la collaboration et le partage des données en toute confiance. Leur principale priorité en matière de sécurité opérationnelle ? La confidentialité des données et la conformité réglementaire.

Dans ce contexte, ce que les DSI recherchent aujourd'hui plus que tout, c'est la certitude que les données métier, RH et financières essentielles ne sont pas seulement conformes, mais aussi protégées contre les cybermenaces et les acteurs internes malveillants. La voie la plus rapide vers ce niveau de confiance est désormais toute tracée. Les leaders technologiques ont besoin d'une stratégie proactive de gestion de la confidentialité des données qui s'appuie sur les meilleures pratiques et une technologie de pointe, et déploie des outils d'automatisation personnalisés qui renforcent les contrôles, la surveillance et les audits.

« Les risques augmentent en même temps que la complexité et l'ampleur des données, souligne Mark Eaglefield, Head of Digital Products chez Veolia UK, un leader mondial des services environnementaux actif dans près de 50 pays. Sans une attitude proactive, il est impossible de quantifier le niveau de risque de l'entreprise, jusqu'à ce que le mal soit fait et que la confiance soit perdue. »

Protéger les données et instaurer la confiance par défaut

Lorsqu'il s'agit des vulnérabilités des multinationales en matière de sécurité des données et de conformité, il peut être difficile de savoir par où commencer. En 2019, les leaders technologiques de Veolia ont pris une décision clé qui a fondé toute sa stratégie de gestion des données : le déploiement intégral de la plateforme Workday.

Pour Mark Eaglefield, un environnement technologique unifié couvrant entre autres la gestion du capital humain, la Finance, la paie et le recrutement a permis d'établir une base de processus bien définis, documentés et gérés concernant l'accès et la sécurité des utilisateurs. « Il s'agit d'une base solide, que nous renforçons avec les meilleures pratiques intégrées dans notre stratégie évolutive et proactive de confidentialité des données », explique-t-il.

Au premier rang de ces pratiques figurent les efforts constants d'éducation et de sensibilisation à la confidentialité des données et à la sécurité des utilisateurs. L'équipe IT de Veolia sensibilise différents groupes d'acteurs impliqués (par exemple les utilisateurs finaux, les auditeurs et les équipes IT) par le biais de sessions de formation, de publications sur les politiques et procédures et de divers canaux de communication.

« Il s'agit d'un cycle continu : l'éducation et la sensibilisation sont essentielles, explique encore Mark Eaglefield. « Nous ne partons jamais du principe que nos acteurs impliqués savent et comprennent comment nous souhaitons protéger les données et quels sont les enjeux. »

Autre bonne pratique adoptée par Veolia : la constitution d'une équipe d'experts internes dédiés à la sécurité. Ces experts, qui maîtrisent parfaitement l'environnement d'exploitation de Workday, collaborent étroitement avec les équipes internes chargées de la protection des données.Ils sont au fait des dernières législations en matière de confidentialité des données et des exigences réglementaires qui en découlent et ont un impact sur l'entreprise.

Ce que les DSI recherchent aujourd'hui plus que tout, c'est la certitude que les données métier, RH et financières essentielles ne sont pas seulement conformes, mais aussi protégées contre les cybermenaces et les acteurs internes malveillants.

45 % des chefs d'entreprise interrogés en Europe ont déclaré qu'ils donneraient la priorité aux dépenses liées à la sécurité des données, à l'atténuation des risques et à la conformité pour soutenir la collaboration et le partage des données en toute confiance.

Ils effectuent une sorte de « révision par les pairs », contribuant à garantir que les politiques, les procédures et les contrôles de l'entreprise reflètent toujours la menace et le paysage réglementaire actuels, indique Mark Eaglefield.

« En ce qui concerne la sécurité et la conformité basées sur les utilisateurs, ces experts sont des collaborateurs essentiels qui nous permettent de renforcer continuellement la conception de notre configuration particulière », explique-t-il.

Des outils adaptés

Chaque entreprise a un environnement de données unique à protéger et des risques associés contre lesquels se prémunir. Chez Veolia, les responsables de la sécurité étaient de plus en plus conscients des vulnérabilités liées à l'accès proxy.

L'entreprise avait mis en place une politique d'accès proxy pour son environnement hors production, qui permettait aux utilisateurs bénéficiant de ce type d'accès de voir toutes les données que les titulaires voient habituellement. Bien que seul un petit nombre de personnes de confiance bénéficiaient d'un tel accès, l'absence de masquage des données exposait Veolia à des risques potentiels de non-respect de la conformité et de violation de la protection des données. L'entreprise a trouvé la parade en adoptant Smart Shield, un outil conçu par Kainos pour permettre le masquage des données pour des utilisateurs proxy spécifiques dans Workday.

« Désormais, nous pouvons nous assurer qu'un utilisateur affecté à un groupe proxy Finance, par exemple, ne puisse pas consulter les données de rémunération de la personne qu'il représente », se réjouit Mark Eaglefield.

Dans les grandes entreprises comptant des milliers, voire des dizaines de milliers d'utilisateurs, il est impossible d'auditer manuellement les configurations des utilisateurs en ce qui concerne la séparation des tâches et les niveaux d'accès au système. L'automatisation des audits doit faire partie de toute solution proactive en matière de confidentialité des données, et c'est pourquoi de nombreux leaders IT s'appuient sur des outils de surveillance de la sécurité à 360 degrés.

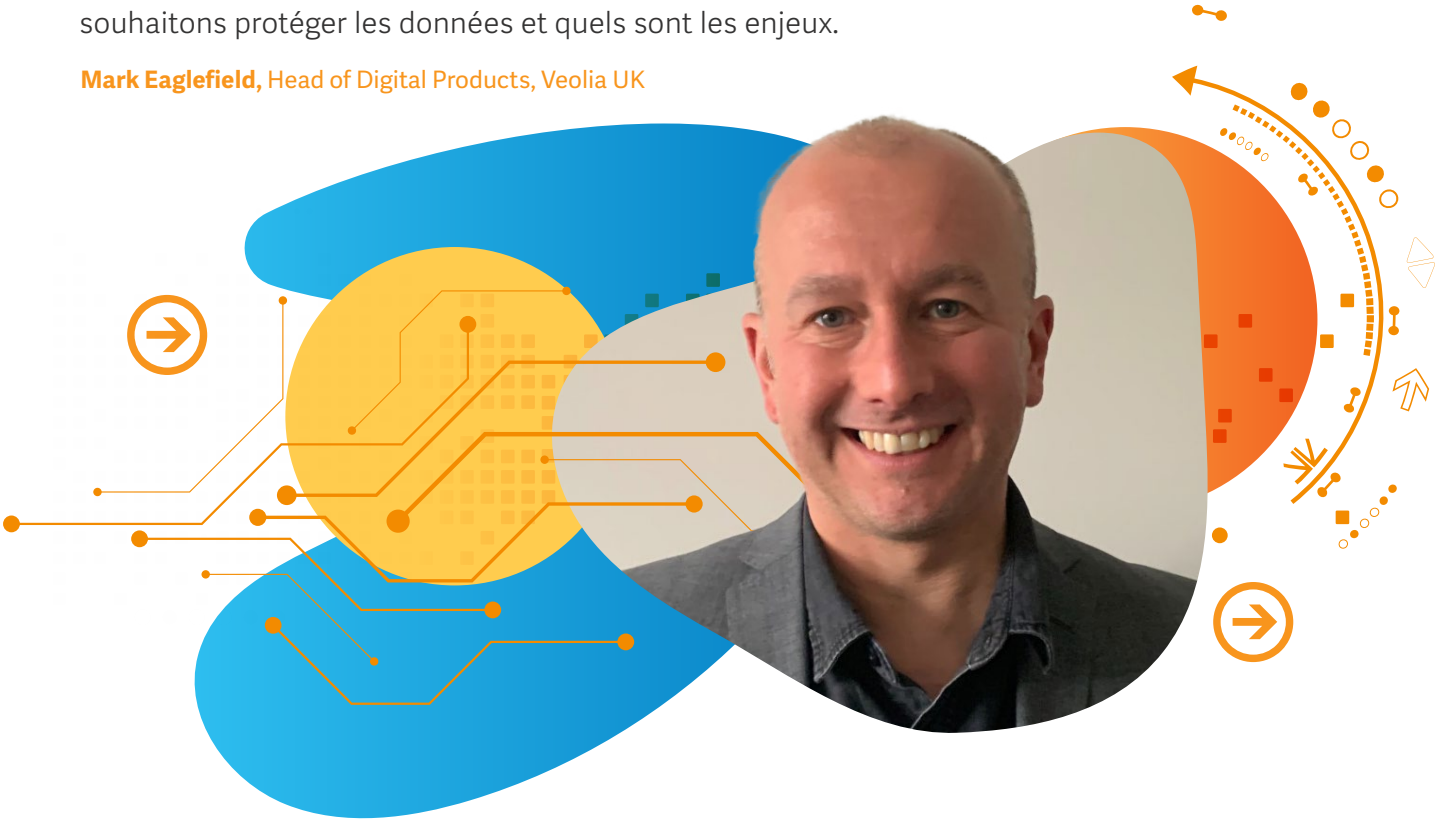
« Plus l'entreprise est complexe, plus il est difficile d'obtenir une vue globale des risques liés aux données, [par exemple] des collaborateurs qui ont un accès inapproprié et illimité à des données très sensibles », avertit Kim Freestone, Product Principal chez Kainos.

Veolia, qui compte 14 000 utilisateurs, a choisi de mettre en œuvre l'outil Smart Audit de Kainos, qui automatise la surveillance de la sécurité des données en signalant notamment les processus de gestion et les données présentant un risque élevé de fraude et de violation. Il est très utile d'avoir un point de vue global, en termes de séparation des tâches et d'identification des conflits associés, note Mark Eaglefield. Des contrôles préventifs permettent de vérifier si le niveau d'accès des utilisateurs aux données est justifié,

> « Plus l'entreprise est complexe, plus il est difficile d'avoir une vue globale des risques liés aux données.
>
> **Kim Freestone,** Product Principal, Kainos

« Nous ne partons jamais du principe que nos acteurs impliqués savent et comprennent comment nous souhaitons protéger les données et quels sont les enjeux.

Mark Eaglefield, Head of Digital Products, Veolia UK



et un e-mail quotidien offre à son équipe de contrôle interne une vue d'ensemble des anomalies, ainsi que le détail des conflits en cours et des processus examinés.

Selon Kim Freestone, l'évaluation proactive des risques ne se limite pas à mettre en place des contrôles et des processus pour protéger les données dans les zones d'accès privilégié. « Il s'agit également de réunir un ensemble de preuves pour montrer aux auditeurs, qu'ils soient internes ou externes, que vous prenez au sérieux l'atténuation des risques », précise-t-il.

Éviter l'autosatisfaction

À l'heure de l'augmentation des menaces de sécurité et de l'émergence de l'IA, la confiance se mérite dans le domaine de la confidentialité et de la protection des données. Cela sera d'autant plus vrai que les entreprises devront à la fois exploiter la puissance de l'IA et se conformer à des cadres réglementaires entièrement nouveaux régissant les ensembles de données et les pratiques, tels que la loi sur l'IA de l'Union européenne.

L'absence de risque n'existe pas lorsqu'il s'agit de données en réseau. Mais avec une stratégie proactive de gestion des données qui englobe à la fois les bonnes pratiques et le meilleur de ce qu'offre actuellement la technologie, les DSI peuvent construire et affiner une infrastructure IT tournée vers l'avenir. Au lieu de s'inquiéter des risques inconnus, les dirigeants peuvent gagner en assurance grâce à un modèle de sécurité hautement configurable régissant l'ensemble des applications et des données de l'entreprise. Les bons outils peuvent mettre en évidence les risques et déclencher les mesures de protection adéquates avant qu'il ne soit trop tard.

Selon Mark Eaglefield, la plus grande erreur en matière de données est l'autosatisfaction : « N'attendez pas qu'un problème survienne, prenez les choses en main dès maintenant. »

Le BYOK pour une protection des données en toute sérénité

En matière de sécurité des données, les attentes des acteurs impliqués, y compris les gouvernements, sont de plus en plus élevées. La possibilité de conserver le contrôle total des clés de chiffrement racine permet d'instaurer la confiance tout en facilitant le respect des réglementations.

Par **Anja Fordon**,
rédactrice EMEA

Si le Cloud computing a transformé la façon dont les entreprises fonctionnent, il a aussi profondément changé la manière dont elles envisagent la sécurité. L'époque où l'on concevait une stratégie de sécurité informatique autour de serveurs et de bases de données sur site est révolue. Le passage à un environnement d'exploitation Cloud, ainsi que l'augmentation de la valeur stratégique des données pour les entreprises, nécessite une approche de la sécurité axée sur les données.

Pour de nombreuses entreprises toutefois, trouver le bon équilibre entre l'agilité de l'informatique dématérialisée et la sécurité des données est un exercice délicat. Cela est particulièrement vrai pour les entreprises des secteurs très réglementés, tels que les services financiers, les services publics et les soins de santé, et celles qui cherchent à se conformer à des réglementations plus strictes en matière de données, telles que le RGPD mis en place par l'UE. Après tout, travailler avec un fournisseur de services Cloud (CSP) implique généralement de confier à ce partenaire des services de chiffrement pour protéger les données des utilisateurs. Cela signifie que, quelle que soit la sécurité de l'environnement Cloud, c'est une autre entreprise qui détient les clés de chiffrement.

Pour les entreprises particulièrement prudentes qui cherchent à renforcer la confiance de leurs clients et à éliminer les problèmes de conformité, une nouvelle solution est apparue ces dernières années : le BYOK (« Bring Your Own Key »).

Pourquoi le BYOK

La valeur fondamentale du BYOK est simple : elle permet à une entreprise de chiffrer ses données dans le Cloud avec sa propre clé de chiffrement racine. L'entreprise peut ensuite autoriser ou refuser l'accès aux données sous-jacentes en partageant la clé racine avec un fournisseur SaaS ou en la révoquant. Il s'agit d'un point de contrôle unique pour l'accès aux données.

« Avec le BYOK, vous avez vraiment le contrôle sur toutes les données de votre entreprise, explique Tammo Buss, Workday Technical Lead chez EWE, une entreprise allemande de services publics dans les secteurs de l'énergie, des télécommunications et des services IT. Plus qu'un simple service de chiffrement, il s'agit d'un service de gestion du chiffrement. »

EWE avait une raison très précise de mettre en œuvre Workday BYOK : assurer la conformité au RGPD. Pour le responsable de la protection des données et l'équipe juridique de l'entreprise, EWE devait avoir un contrôle total sur ses propres données dans un environnement Cloud. Selon Tammo Buss, un avantage spécifique du BYOK dans le secteur hautement réglementé d'EWE est lié aux audits des données des clients.

« Il est formidable que nous disposions d'un produit dans lequel tout est très transparent, ce qui nous permet de rationaliser l'audit de sécurité et la réponse de conformité », se réjouit Tammo Buss. En décembre 2023, EWE a mis en service diverses solutions Workday, dont Workday BYOK.

Au-delà des audits de conformité, l'avantage principal du BYOK est le contrôle total de l'accès à vos données.

La valeur fondamentale du BYOK est simple : elle permet à une entreprise de chiffrer ses données dans le Cloud avec sa propre clé de chiffrement racine.

Contrôle total

En général, le BYOK peut être mis en œuvre de plusieurs façons. La manière dont une entreprise gère ses clés de chiffrement racine dépend non seulement de sa propension au risque et de sa capacité à gérer les clés en interne, mais également du service de gestion des clés sous-jacent du CSP.

Par exemple, un CSP peut être en mesure d'utiliser une clé de chiffrement racine générée en dehors de son système, mais il a besoin que le client charge les clés sur ses serveurs. Cette approche pourrait permettre à un CSP de gérer certaines tâches de gestion du chiffrement, telles que la rotation des clés racine pour le compte du client, ce qui donne le contrôle du chiffrement de la racine au fournisseur de services et non au client.

EWE a toutefois pu conserver le contrôle total de tous les aspects de sa clé de chiffrement racine, car Workday BYOK permet au client de posséder et de gérer entièrement cette clé en dehors de Workday. EWE a mis en place un service de gestion des clés géré par le client dans AWS, avec lequel le compte Workday d'EWE est ensuite interfacé.

« Grâce à cette approche de clé gérée par le client, nous avons pu chiffrer toutes nos données Workday et tous nos tenants avec notre propre clé et en avoir le contrôle total », explique Tammo Buss.

Le fournisseur AWS a certifié qu'à aucun moment il ne peut accéder à une clé générée par un client, qu'elle soit utilisée dans son système de gestion des clés ou dans un module de sécurité hybride, le système de traitement cryptographique qui protège les clés digitales. « Il s'agit d'un aspect important pour prouver la conformité lors des audits SOC (System and Organisation Control), souligne Tammo Buss. Notre conseiller juridique a été très satisfait de la documentation fournie. »

Plus grande responsabilité et ROI tangible

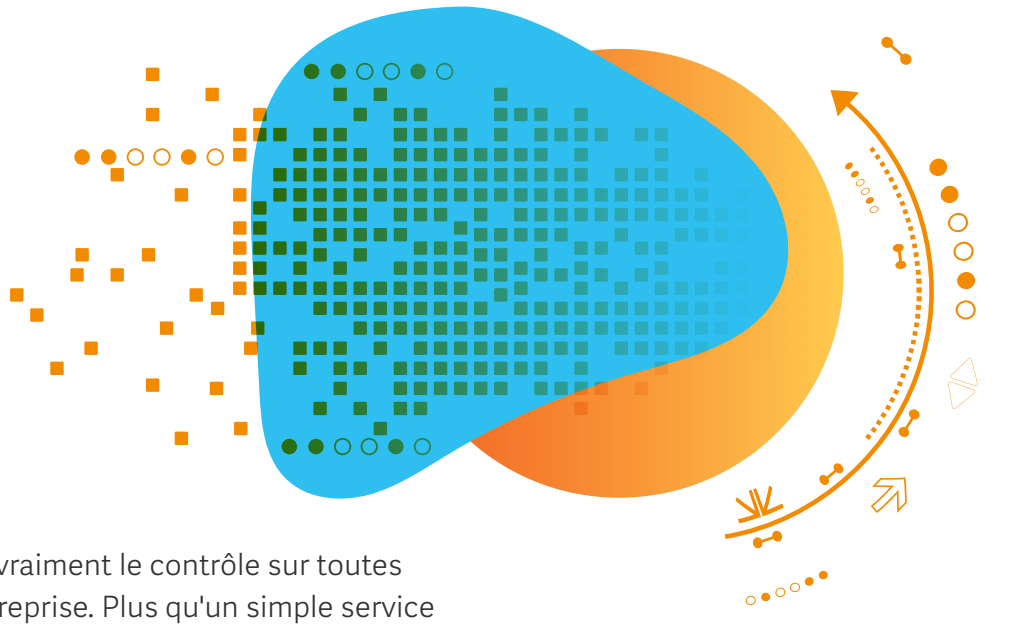
Si Workday BYOK apporte une valeur ajoutée évidente en termes de conformité et d'amélioration de la sécurité des données, les entreprises qui envisagent de mettre en place le modèle doivent toutefois bien réfléchir aux éventuelles difficultés.

La plus évidente est que le BYOK implique de plus grandes responsabilités, ce qui peut entraîner des dépenses supplémentaires. L'équipe IT interne de l'organisation peut être amenée à gérer un compte AWS, mais si un partenaire externe a besoin d'accéder à la clé racine, elle devra s'occuper de lui fournir l'accès. Un fournisseur de services IT pourrait également se charger de certaines tâches liées au BYOK, mais une telle délégation va à l'encontre de l'objectif principal du modèle.

Et si l'entreprise perd la clé principale ? Il s'agit là d'un vrai problème.

« Il n'y a pas de solution de secours, rappelle Gautam Roy, Principal Product Manager chez Workday, qui s'est occupé du compte Workday d'EWE. Si le client révoque l'accès à la clé racine, Workday perd l'accès aux données. C'est le principe même du BYOK. Nous ne faisons pas de sauvegarde des clés. Nous avons besoin d'accéder en temps réel aux données par le biais des clés racine ».

> « De notre point de vue, le coût de la mise en œuvre et de la maintenance est en fait assez faible. La solution est facile à utiliser et à maintenir, et nous avons considérablement réduit les risques liés à la sécurité des données.
>
> **Tammo Buss,** Workday Technical Lead, EWE



« Avec le BYOK, vous avez vraiment le contrôle sur toutes les données de votre entreprise. Plus qu'un simple service de chiffrement, il s'agit d'un service de gestion du chiffrement.

Tammo Buss, Workday Technical Lead, EWE

Pour EWE, le surcroît de travail et de responsabilités lié au BYOK en valait la peine. L'entreprise a choisi d'éliminer le risque de non-conformité au RGPD au moyen d'une solution technique, plutôt que de le réduire par le biais d'un accord contractuel sur la confidentialité des données. D'après Tammo Buss, toutes les entreprises européennes, et en particulier celles qui opèrent dans des secteurs très réglementés, doivent se préoccuper des risques liés à la confidentialité des données, tout en gardant à l'esprit que les cadres réglementaires ne cesseront d'évoluer. Avec la prochaine réglementation de l'UE sur l'IA, les entreprises doivent se préparer à être agiles en ce qui concerne les pratiques de sécurité des données.

Workday BYOK peut s'avérer très utile à cet égard. « Nous sommes ravis d'avoir mis en place le BYOK, car lorsque les exigences de conformité évoluent, nous savons que nous gardons le contrôle technique de nos données, indique Tammo Buss.

Cela devrait réduire la nécessité de réunir les équipes juridiques pour mettre à jour les accords sur la confidentialité des données avec de nouvelles parties contractuelles. »

Ainsi, si le BYOK engendre des coûts, il peut aussi réduire le coût des activités futures liées à la conformité, tout en contribuant à prévenir de coûteuses failles de sécurité des données.

« De notre point de vue, le coût de la mise en œuvre et de la maintenance est en fait assez faible, estime Tammo Buss. La solution est facile à utiliser et à maintenir, et nous avons considérablement réduit les risques liés à la sécurité des données. »

Au-delà des audits de conformité, l'avantage principal du BYOK est le contrôle total de l'accès à vos données.

Nous contacter

SOUMETTEZ-NOUS vos idées de sujets, **RÉDIGEZ** vos propres articles pour le magazine ou **ABONNEZ-VOUS** pour rejoindre la communauté smartCIO et recevoir l'édition digitale trimestrielle ainsi que des infos sur les événements locaux.

Tout ceci via une seule adresse.

Écrivez-nous à **smartcioemea@workday.com**

Workday | Téléphone : +33 (0)1 84 88 34 44 | workday.com/fr