Communiqués de presse

Que signifie pour les entreprises l'évolution de l'Europe vers un Cloud de confiance ?

Par Agnieszka Bruyère, Vice-Présidente IBM Cloud, IBM EMEA, le 21 juin 2021 : L'instauration de la confiance dans le Cloud est au cœur d'un nouveau mouvement en Europe visant à générer de la valeur à partir des données et des innovations technologiques. Les vastes mines de données industrielles de l'Europe se sont encore agrandies en raison de la numérisation accélérée pendant le confinement mondial.

À une époque où les innovations dans le domaine des technologies de l'information connaissent une croissance rapide, il est essentiel d'en tirer des bénéfices pour relever les défis de la société, des organisations et des entreprises. La véritable valeur réside dans les solutions et les services qui permettent de relever ces défis. Cela nécessite une approche multidisciplinaire, basée sur un écosystème. L'ensemble des initiatives européennes de souveraineté devraient encourager et renforcer toute forme de collaboration tirant parti des innovations technologiques existantes afin de créer des cas d'usage pertinents pour les différents secteurs et la société dans un climat de confiance.

Explorons les enjeux de la souveraineté numérique et certaines des initiatives menées par les gouvernements et les fournisseurs de services Cloud et montrons comment les organisations peuvent en bénéficier.

Une souveraineté numérique gagnante

La souveraineté numérique est une approche menée par l'Union Européenne. Elle peut prendre de nombreuses formes. Nous présentons ici cinq piliers essentiels à sa réussite :

- **Autonomie stratégique**. Permettre aux organisations européennes de créer de nouveaux business et de nouveaux services pour les clients et les citoyens en exploitant les technologies existantes de manière sécurisée et fiable et en tirant parti de l'énorme quantité de données européennes. Cela nécessite 1) la confiance numérique (protection des données, cyber-résilience, valeurs partagées), 2) la capacité d'adopter la technologie, incluant toutes les innovations, plutôt que de réinventer la roue, et 3) une approche basée sur un écosystème de l'ensemble des parties prenantes : ceux qui comprennent les défis d'un secteur d'activité (par exemple, la finance, la santé, l'industrie, etc.), ceux qui fournissent la technologie et ceux qui peuvent la mettre en œuvre.

- **Stimuler l'innovation grâce à une approche basée sur un écosystème.** L'approche basée sur un écosystème est non seulement nécessaire pour unir les forces de différents types de parties prenantes (industries, fournisseurs de technologies, intégrateurs de systèmes) mais également pour rassembler les représentants d'une même industrie (secteur) dans des espaces de confiance pour accéder aux données et les partager ainsi que pour collaborer afin de permettre l'invention de nouveaux services (par exemple, pour la lutte contre la fraude).

- **Protection accrue des données personnelles et industrielles et de la propriété intellectuelle.** La transformation numérique et la garantie d'une économie des données sûre et sécurisée ne s'excluent pas mutuellement. Le défi consiste à permettre aux organisations d'atteindre plus facilement un niveau élevé de protection des données. Ce haut niveau de protection des données peut être atteint grâce à un

engagement contractuel, des certifications et des technologies de sécurité avancées, des mesures de sécurité et des contrôles et rapports de conformité en temps réel. Ces normes élevées de sécurité et de protection doivent s'appliquer aux données (en particulier aux données sensibles). Les organisations doivent garder le contrôle total et la propriété non seulement de leurs données mais également des connaissances qui en découlent pour stimuler l'innovation.

- **Amélioration de la cybersécurité.** L'année dernière encore, nous avons observé un nombre record d'incidents de sécurité qui ont eu des répercussions sur les données et les opérations des entreprises, paralysant ainsi les sociétés et les organisations. Bien que le Cloud apporte un ensemble de mesures de sécurité combinées à un certain nombre de certifications pour garantir un niveau élevé de normes de sécurité, la répartition des responsabilités entre les fournisseurs de Cloud et les utilisateurs peut introduire une certaine confusion ou ambiguïté. La clarté et le bon niveau de sensibilisation des utilisateurs sont essentiels pour garantir la cyber-résilience. La clarté doit reposer sur deux piliers :
  - La cyber-résilience des fournisseurs de services Cloud (CSP), souvent appelée « security below the line » se compose d'un ensemble de mesures, de processus et de contrôles de sécurité ainsi que de services de sécurité spécifiques auxquels les utilisateurs peuvent souscrire. Le niveau de cyber-résilience des CSP se mesure par un ensemble de certifications obtenues (telles que les certifications ISO liées à la sécurité, la certification SOC2 et toute certification spécifique par secteur) ainsi que par tout autre outil de contrôle spécifique au secteur (tel que le centre de sécurité et de conformité d'IBM pour les services financiers).
  - La cyber-résilience dite « above the line » concerne les mesures spécifiques que les clients doivent mettre en place pour compléter la cyber-résilience des fournisseurs de Cloud. Les utilisateurs du Cloud sont tenus de souscrire à des services spécifiques adaptés aux exigences de sécurité de leur environnement (par exemple, les services Hyper Protect d'IBM avec module cryptographique de niveau 4) et de mettre en place un suivi et un contrôle global de la sécurité.

- **Une nouvelle génération de talents.** Former, requalifier, et renforcer les compétences des étudiants et des professionnels pour développer et déployer les infrastructures et les services nécessaires à l'économie des données.

Il existe un certain nombre d'initiatives visant à atteindre les objectifs de la souveraineté numérique.

L'EU Cloud Code of Conduct - l'assurance des normes de confidentialité et de sécurité les plus élevées dans le Cloud

IBM a joué un rôle de premier plan dans l'élaboration du code de conduite de l'UE en matière de protection des données pour les fournisseurs de services Cloud et a été le premier à adhérer à ce code pour ses services en 2017.

Le Code est contrôlé de manière indépendante et contient des garanties rigoureuses, notamment les mesures de conformité au RGPD, pour la protection des données dans les services Cloud.

L'EU Cloud Code of Conduct a reçu l'approbation officielle de l'autorité principale de protection des données. Cette approbation garantit et prouve que les services souscrits sont non seulement conformes au RGPD, mais

vont encore plus loin en termes de confiance, de responsabilité et de transparence.

Grâce au Code de conduite, les utilisateurs de Cloud exploitant un service Cloud qui adhère au Code peuvent être sûrs qu'ils respectent le RGPD et que leurs données sont sécurisées.

GAIA-X - une infrastructure Cloud européenne

GAIA-X conduira à la prochaine génération d'infrastructure de données en Europe : une coopération entre les pays européens et les entreprises de Cloud sur un système Cloud fédéré qui permet aux organisations d'exploiter les avantages du Cloud computing et de collaborer avec des partenaires sans être « verrouillées » par des fournisseurs. IBM est membre de GAIA-X. Nous partageons ses objectifs en matière de responsabilité, de sécurité et de protection des données mais également d'interopérabilité, de portabilité, et de la promotion de normes et environnements ouverts.

Fournir des garanties techniques

Pour faire partie de l'économie des données digne de confiance, les organisations doivent avoir le choix entre les meilleures solutions de protection de la vie privée et de sécurité. La priorité d'IBM est de fournir des technologies de préservation de la confidentialité uniques en leur genre afin de favoriser le partage des données au sein des organisations et entre elles. Certaines de nos dernières innovations aideront les organisations à faire partie d'une économie européenne des données basée sur la confiance :

- *Le confidential computing*
  Notre capacité de confidential computing (informatique confidentielle) constitue une véritable avancée. Pendant des années, les fournisseurs de Cloud n'ont pu proposer que des services de chiffrement qui protégeaient les données « au repos » et « en transit », laissant les données « en cours d'utilisation » vulnérables. Le confidential computing d'IBM chiffre et protège en permanence les données tout au long de leur cycle de vie informatique, y compris lorsqu'elles sont traitées en mémoire. Cette approche globale de la protection des données ouvre de nouvelles possibilités passionnantes pour tirer parti de l'innovation dans le Cloud et répond avec succès à certaines des préoccupations en matière de sécurité et de confidentialité.

- *Le « Keep your own key »*
  Le « Keep your own key » est une technologie de chiffrement de pointe qui permet aux entreprises de garder le contrôle de leurs propres clés de chiffrement, ce qui signifie qu'elles sont les seules à pouvoir contrôler l'accès à leurs données. Le leadership d'IBM dans ce domaine est soutenu par le plus haut niveau de certification de sécurité disponible sur le marché.

- *Le Cloud hybride*
  Le nouveau paradigme du Cloud hybride permet aux utilisateurs de bénéficier des innovations technologiques (généralement nées dans le Cloud) dans n'importe quel modèle de déploiement -

Cloud public, en local, à la périphérie (at the edge). Aujourd'hui, le Cloud hybride ne consiste plus à connecter l'informatique du datacenter local au Cloud public, mais à apporter véritablement des services Cloud là où l'organisation le décide, avec tous les modèles opérationnels possibles : sous forme de licence (gérée par les clients) ou géré par le fournisseur de Cloud. L'approche Cloud hybride d'IBM, qui s'appuie largement sur les open sources, offre une portabilité et une liberté totale de choix en termes de déploiement et de modèles opérationnels.

- *EU-only services*
  Les services EU-only permettent aux clients de stocker et de traiter des données dans l'Union européenne. L'option EU-only d'IBM garantit que les données des clients sont stockées et traitées dans l'Union européenne et que ce sont des professionnels basés dans l'UE qui effectuent les mises à jour et opèrent les services Cloud. Si un personnel non européen doit accéder à l'infrastructure ou à un service (par exemple, pour un incident de niveau 3 qui ne peut être résolu par les professionnels de l'UE), l'autorisation d'accès est soumise à un processus d'approbation et à des contrôles stricts.IBM dispose de capacités étendues et inégalées de stockage et de traitement des données dans l'UE. Nous fournissons un support réservé à l'UE pour nos services Cloud depuis 2017 (avant le RGPD). Notre infrastructure Cloud à Francfort est certifiée C5 par l'agence allemande de cybersécurité BSI.

Conclusion

La confiance et la transparence sont fondamentales pour exploiter pleinement le potentiel de l'économie des données. L'accent mis par l'Europe sur le Cloud de confiance crée de nouvelles opportunités pour les entreprises.

IBM soutient les efforts de l'UE visant à instaurer une plus grande confiance dans l'économie numérique et à devenir un chef de file d'une révolution numérique fondée sur les valeurs. IBM participe depuis des années à des initiatives de l'UE (entre autres : l'EU Cloud Code of Conduct et GAIA-X) pour contribuer à instaurer la confiance numérique. IBM adhère aux valeurs européennes et se conforme aux réglementations de l'UE et aux normes de sécurité les plus élevées.

Comme l'a redit récemment Martin Jetter, Président d'IBM EMEA, notre engagement est et a été très clair. Les entités européennes d'IBM sont soumises à leur juridiction nationale et rejetteront toute demande d'autorités n'ayant aucune juridiction sur elles d'accéder aux données qui leur sont confiées par une entreprise ou une organisation.

IBM est là pour soutenir l'UE dans son travail, pour tenir nos clients au courant des évolutions et pour les aider à générer de la valeur à partir de leurs données.

Contacts presse :

Weber Shandwick pour IBM

IBM
Gaëlle Dussutour
Tél. : + 33 (0) 6 74 98 26 92
dusga@fr.ibm.com

Robin Legros / David Boutet

Tél. : + 33 (0)6 68 04 57 83 / +33 (0)6 6 63 45 03 79

ibmfrance@webershandwick.com