

CII WHITE PAPER

Entre quasi-monopole et « sovereignty washing » :

les obstacles à la mise en place d'une infrastructure cloud souveraine pour l'administration allemande

Michael Kolain, *Senior Fellow au cyberintelligence.institute*



CYBER|INTELLIGENCE
.institute

Contenu

Résumé	3
Introduction	5
Le statu quo – L’empire Microsoft et son contexte	7
I. Le pouvoir de Microsoft sur le marché du secteur public et ses causes	7
II. Propriétaire, peu sûr, illégal ? – Critiques à l’égard de l’utilisation de Microsoft dans l’administration	11
L’informatique ne peut pas vivre – avec ou sans Microsoft ?	
Un cloud « souverain », s’il vous plaît !	15
Adaptations de produits et offres de Microsoft entre efforts sérieux et « sovereignty washing »	17
I. Programme européen de sécurité	17
II. Conditions de protection des données négociées individuellement	17
III. La solution Delos : faire exploiter les centres de données par des entreprises européennes – (seuls) les logiciels proviennent de Microsoft	18
IV. Limite des données et instances locales	19
Résumé et recommandations d’action	21
Mesures à court terme jusqu’en 2028	22
Mesures à moyen terme pour les négociations du prochain contrat-cadre du BMI	23
Mesures à long terme pour l’ère de la souveraineté numérique dans l’UE et en Allemagne	24

L’auteur

Michael Kolain, Senior Fellow

Michael Kolain est juriste et expert en politique numérique. Au FÖV Speyer, il a mis en place le programme « Numérisation » au sein de l’équipe du professeur Mario Martini et mené des recherches sur la réglementation de l’IA, la numérisation de l’administration et le droit des données (et de leur protection). En tant que conseiller parlementaire pour la politique numérique, il a participé à l’élaboration de la législation du gouvernement de coalition. Il travaille à l’interface entre la législation, la science et le développement des technologies numériques.



Résumé

L'administration publique allemande dépend de facto de Microsoft dans des domaines clés de son informatique. Grâce à des écosystèmes fermés, à des offres groupées de produits ciblées, à une gestion restrictive des licences et à un lobbying massif, le groupe a établi une position de quasi-monopole. Celle-ci fait systématiquement obstacle à une concurrence ouverte, libre et équitable sur le marché européen du cloud.

Il en résulte une liberté de choix limitée, des risques de sécurité croissants, un manque de transparence et une perte de souveraineté budgétaire dans les finances publiques. Les effets de verrouillage agissent ici comme un levier : les normes propriétaires, l'étroite interdépendance entre le client, le serveur et le cloud, ainsi que les coûts élevés de migration vers des solutions alternatives maintiennent les autorités dans l'écosystème Microsoft. Malgré la diversité des offres existantes, les alternatives souveraines sur le plan numérique n'ont pratiquement aucune chance. Parallèlement, l'abandon annoncé des licences sur site à durée indéterminée et le passage à des modèles d'abonnement obligatoires avec connexion Azure à partir de 2029 renforcent cette dépendance. Les prix et les conditions passent sous le contrôle de Microsoft, avec les risques liés aux devises et à l'escalade.

Cette configuration est toxique pour la souveraineté numérique de l'administration publique. L'État perd le contrôle du code, de la politique de mise à jour et des flux de données.

Cette configuration est toxique pour la souveraineté numérique de l'administration publique. L'État perd le contrôle du code, de la politique de mise à jour et des flux de données. En effet, Microsoft protège les composants centraux en tant que secrets commerciaux et déploie des mises à jour mondiales qui ne peuvent être ni auditées de manière exhaustive au préalable, ni suffisamment adaptées aux besoins individuels des autorités allemandes. Les incidents de sécurité de ces dernières années, du désastre de la chaîne d'approvisionnement aux violations de la protection des données, ont montré à quel point un modèle cloud centralisé est vulnérable : chaque faiblesse

au cœur du système se répercute à la périphérie et rend l'administration potentiellement vulnérable. À cela s'ajoutent des incertitudes juridiques et de conformité, notamment en raison du traitement opaque des données de diagnostic, de la domination extraterritoriale des données et de la vérifiabilité limitée de ce qui se passe exactement lors des accès à distance pour la maintenance des systèmes. Même les modèles d'exploitation apparemment souverains n'y changent pas grand-chose : les variantes de conception partiellement souveraines avec des centres de données nationaux ou des « frontières de données de l'UE » s'attaquent aux symptômes, pas aux

Tant que le code, les mises à jour et le contrôle de l'architecture sont localisés dans un seul groupe, les dépendances juridiques et techniques persistent.

causes. Tant que le code, les mises à jour et le contrôle de l'architecture sont localisés dans un seul groupe, les dépendances juridiques et techniques persistent ; les prix plus élevés de ces « coquilles de sécurité » sans véritable indépendance aggravent encore le contrôle des coûts.

En matière de politique concurrentielle, Microsoft modifie la logique du marché en regroupant stratégiquement certains produits et en créant des réseaux de distribution étroitement liés : lorsque l'outil de communication Teams est en fait « fourni » et que les interfaces ne sont pas suffisamment ouvertes, les alternatives interopérables perdent de leur attrait. Des décennies de lobbying, des structures de partenariat denses et des contrats cadres pluriannuels renforcent cette domination et compliquent la tâche des acheteurs publics qui souhaitent ancrer des architectures modulaires indépendantes des fabricants

dans la salle des machines numérique. Il en résulte un cercle vicieux numérique : les responsables politiques réagissent à la viabilité à court terme, le marché s'adapte à la domination et la capacité stratégique de l'État à contrôler de manière autonome son environnement informatique diminue.

Cette situation n'est pas compatible avec l'objectif politique de souveraineté numérique. En effet, la souveraineté numérique nécessite une véritable liberté de choix, tant sur le plan technique que juridique et économique. Le cycle actuel de l'accord-cadre entre le ministère fédéral de l'Intérieur et Microsoft, qui court jusqu'en 2028 et qui constitue la base de la plupart des processus d'approvisionnement au niveau fédéral, régional et local, doit être utilisé comme une phase de transition pour planifier et mettre en œuvre un abandon progressif des dépendances informatiques monolithiques. Cela comprend : l'ancrage obligatoire de normes et d'interfaces ouvertes dans les futurs contrats (portabilité, interopérabilité, règles de sortie), des architectures de référence multi-constructeurs avec des critères de charge de travail clairs au lieu d'une obligation de cloud, des audits obligatoires avec accès au code dans le respect de la confidentialité, une journalisation immuable et vérifiable en continu de tous les accès à distance, la souveraineté des autorités en matière de clés et des bilans fiables des coûts et des dépendances à tous les niveaux administra-

donnée au niveau de l'UE, qui positionne l'Allemagne comme client de référence et regroupe le pouvoir de négociation des pouvoirs publics à l'échelle transnationale. La France et l'Allemagne devraient profiter du « Sommet sur la souveraineté numérique 2025 » le 18 novembre 2025 pour poser les jalons décisifs d'un cloud administratif souverain digne de ce nom.

Le secteur public doit montrer l'exemple : réduire activement dès maintenant les dépendances existantes vis-à-vis de Microsoft, mettre en place des projets pilotes et des voies de migration vers des solutions ouvertes et interopérables, financer le développement des compétences et miser strictement sur des solutions modulaires dans les marchés publics. La souveraineté numérique n'est pas un label de relations publiques, mais une mission de contrôle de l'État : elle résulte d'un leadership politique, d'une mise en œuvre technique et d'une application concurrentielle. Ceux qui misent aujourd'hui de manière cohérente sur des écosystèmes ouverts réduiront demain les risques liés à la sécurité et à la chaîne d'approvisionnement, renforceront leur souveraineté budgétaire et créeront une base informatique solide et viable à l'échelle européenne. Car seul un État qui maîtrise et contrôle de manière souveraine ses bases de travail, ses infrastructures et ses processus de communication est résilient face aux menaces extérieures.

L'État lui-même doit ici prendre les devants, au lieu de se laisser séduire par les promesses d'un « lavage de souveraineté », comme le résume la Société allemande d'informatique.

tifs. L'État lui-même doit ici prendre les devants, au lieu de se laisser séduire par les promesses d'un « **lavage de souveraineté** », comme le résume la *Société allemande d'informatique*. Les procédures d'examen en matière de droit des ententes devraient examiner en détail toutes les pratiques en matière de licences et de regroupement qui suppriment de facto la liberté de choix et y remédier par des mesures réglementaires appropriées. Parallèlement, les États membres de l'UE sont appelés à promouvoir de manière ciblée des alternatives européennes et ouvertes, par le biais de consortiums, de mises en œuvre de référence et d'une stratégie d'approvisionnement coordonnée.

Chapitre 1 : Introduction

Quand on entre dans un bureau administratif allemand, on ne trouve pas seulement des piles de dossiers, des trombones et des tampons sur les bureaux. On trouve aussi, comme dans la plupart des bureaux allemands, des ordinateurs. Même si, du point de vue des citoyens qui communiquent (souvent par la poste) avec l'administration, la situation semble parfois différente, les routines de travail de l'administration publique se sont largement numérisées au cours des dernières décennies. Sans matériel et logiciels, la plupart des administrations ne seraient plus en mesure de fonctionner aujourd'hui. Mais avec l'augmentation des équipements numériques, des relations commerciales intensives se sont développées avec des prestataires informatiques privés. Au niveau des logiciels, **le groupe Microsoft domine l'administration numérique**.

Tout employé de l'administration publique qui allume un ordinateur public verra généralement le logo du système d'exploitation Windows. Quiconque prépare un acte administratif ou rédige des notes utilisera la suite Office de Microsoft : *Word* pour les textes, *Excel* pour les tableaux, *PowerPoint* pour les présentations. La maîtrise des applications Microsoft est une compétence requise dans presque toutes les offres d'emploi de la fonction publique. Mais lorsqu'il s'agit d'équiper l'administration et d'assurer sa capacité de travail, il devrait être exclu, ou du moins rare, de dépendre d'un seul fournisseur, sauf pendant une période transitoire. Il est tout à fait naturel que l'administration achète du papier pour imprimantes, des bureaux, des ordinateurs portables et des armoires de classement sur le marché, en choisissant différents fabricants proposant les meilleurs prix et les meilleures offres. L'État reste ainsi indépendant des différents fournisseurs et peut toujours conserver une certaine flexibilité dans ses procédures d'achat. Cependant, presque tous les budgets des communes, des Länder et des ministères fédéraux comportent des licences Microsoft pour un montant considérable dans la partie débitrice du budget, tandis que les fournisseurs alternatifs et les concurrents mènent une existence discrète.

Le fait que l'administration soit pour ainsi dire sous la coupe d'un groupe qui, **selon l'Office fédéral des cartels**, a une « importance prépondérante pour la concurrence sur l'ensemble du marché » peut entrer en conflit avec **le principe constitutionnel** selon lequel l'administration doit exercer ses fonctions de manière indépendante et conformément aux dispositions légales. Que pourrait faire le gouvernement fédéral si Microsoft campait sur ses positions lors d'une renégociation du contrat-cadre du BMI et doublait ou triplait simplement ses prix ? La réponse à cette question est d'autant plus pertinente que, en Allemagne, Microsoft est le seul groupe à détenir et à maintenir un monopole sur les logiciels de productivité dans le cloud, empêchant ainsi de manière ciblée le passage à d'autres fournisseurs dans un marché libre, ouvert et interopérable.

Malgré les bouleversements géopolitiques, l'Allemagne est sur le point, en 2025, d'approfondir encore sa coopération avec Microsoft, bien que le groupe américain mène une politique commerciale visant à rendre l'État encore plus dépendant de ses services.

Malgré les bouleversements géopolitiques, l'Allemagne est sur le point, en 2025, d'approfondir encore sa coopération avec Microsoft, bien que le groupe américain mène une politique commerciale visant à rendre l'État encore plus dépendant de ses services. De plus, le groupe de Redmond souhaite inciter ses utilisateurs à ne plus acheter ses logiciels standard, d'Outlook à Teams en passant par PowerPoint, via des licences individuelles à durée illimitée, mais à les utiliser uniquement en connexion avec le cloud Azure de Microsoft. Les autres connexions aux programmes Office devraient être supprimées d'ici 2029, en particulier les licences logicielles dites « sur site ».

Bien qu'il existe sur le marché certaines alternatives à Windows, Office, Microsoft365 et Azure et que les premiers acteurs publics se tournent déjà vers d'autres

applications, Microsoft reste le leader incontesté de l'informatique publique, tant dans les États membres que dans l'UE. Une **étude récente de l'Open Cloud Coalition** a une nouvelle fois souligné la part de marché dominante de Microsoft dans le domaine des logiciels de bureau (*Office*, 90 %) et de *la collaboration* (84 %). Une part de marché élevée, supérieure à 80 %, génère bien sûr des revenus importants pour ce quasi-monopole : selon les dernières estimations, 198 millions d'euros provenant des contribuables allemands ont été versés à Microsoft pour des licences Office et des systèmes d'exploitation. Microsoft réinvestit ces bénéfices dans des activités de lobbying intensives qui continuent de programmer le régime de licences et la logique produit pour créer des dépendances ciblées et durables.

Il existe différentes propositions pour remédier à la dépendance de l'administration allemande vis-à-vis de Microsoft : d'une sortie stratégique de l'écosystème Microsoft à une date butoir donnée, en passant par une part obligatoire d'open source dans les marchés publics informatiques, l'exploitation de la gamme de produits Microsoft avec stockage des données administratives par une entreprise allemande, jusqu'à des mesures et obligations de sécurité strictes garanties contractuellement par Microsoft lui-même.

Sous l'influence de la situation géopolitique actuelle, l'Allemagne et de nombreux autres gouvernements de l'UE aspirent politiquement à un état de « souveraineté numérique ». Une grande partie de ce débat se concentre sur la promotion de l'infrastructure et de l'industrie numériques dans l'UE. Si ces efforts sont louables sur le plan politique abstrait, leur mise en œuvre concrète nécessite beaucoup de temps, des stratégies claires et des investissements importants. Se libérer des dépendances qui se sont développées au fil des décennies est un effort de longue haleine. Le livre blanc met en évidence les obstacles à la souveraineté numérique et ce qui serait politiquement possible dans le contexte technologique actuel pour aider l'administration à bénéficier d'une plus grande liberté de choix concernant son environnement de travail numérique.

Dans ce livre blanc, nous décrivons à quel point les autorités et les entreprises européennes sont devenues dépendantes de certains produits Microsoft et nous mon-

trons les inconvénients que cela comporte pour l'État et l'économie (**chapitre 2**). Au **chapitre 3**, nous retraçons les activités du groupe Microsoft en matière de lobbying et de développement de modèles commerciaux, qui visent à maintenir sa position de monopole de fait sur les systèmes d'exploitation et les logiciels standard utilisés dans les environnements de travail numériques publics. Au **chapitre 4**, nous recherchons des scénarios susceptibles d'ouvrir la voie entre le statu quo et l'objectif politique d'une « infrastructure cloud souveraine » en Allemagne et en Europe. Enfin, nous formulons des recommandations d'action à l'intention des décideurs politiques (**chapitre 5**).

Souveraineté numérique

ne vise pas l'autosuffisance ou l'isolationnisme numérique, mais vise à donner à l'État la possibilité de garantir la liberté de choix technologique et de concevoir son environnement de travail numérique conformément à sa stratégie et à la législation. Cet objectif ne peut être atteint en recherchant l'indépendance vis-à-vis des fournisseurs non européens, c'est-à-dire en recourant uniquement à des entreprises européennes ou allemandes. La souveraineté numérique signifie plutôt réduire les pratiques qui privent l'État de sa liberté de choix en matière d'infrastructure numérique. La souveraineté numérique signifie que les conditions d'un environnement de marché équitable sont réunies, dans lequel les clients ont un véritable choix entre les fournisseurs de logiciels et de services cloud à l'intérieur et à l'extérieur de l'Europe. Dans le meilleur des cas, l'État compose son environnement informatique de manière modulaire et en fonction de ses besoins à partir de composants interopérables qui communiquent entre eux via des interfaces ouvertes. Le contraire de la souveraineté numérique, ce sont les dépendances de fait vis-à-vis de quasi-monopoles et un « kill switch » à l'étranger qui peut surveiller ou paralyser complètement le travail administratif numérique.

Chapitre 2 :

Le statu quo – L'empire Microsoft et son contexte

Le groupe informatique fondé par Bill Gates en 1975 aux États-Unis sait, à l'aube de l'ère proclamée du cloud, comment fidéliser, maintenir et renforcer la fidélité de ses clients. C'est le fruit d'années de marketing intensif et de lobbying de la part du groupe dont le siège social se trouve à Redmond, aux États-Unis. Il est dans l'intérêt

Il est dans l'intérêt économique légitime d'un groupe informatique internationalement prospère de consolider et d'étendre sa part de marché dans le secteur public.

économique légitime d'un groupe informatique internationalement prospère de consolider et d'étendre sa part de marché dans le secteur public. Il n'est donc pas surprenant que ces nouvelles offres s'inscrivent dans une stratégie délibérée : si les autorités publiques misent déjà largement sur Microsoft, pourquoi ne pas conquérir d'autres segments de l'informatique publique ?

I. Le pouvoir de Microsoft sur le marché du secteur public et ses causes

Une [étude récente de l'Open Cloud Coalition](#) a analysé la part de marché dominante du groupe Microsoft dans le domaine des logiciels standard par rapport à *Amazon Web Services* et *Google* : dans le domaine « Office », les auteurs ont calculé une part de marché de 90 %, contre 84 % dans le domaine « Collaboration ». C'est pourquoi le livre blanc se concentre sur « l'acteur le plus puissant du marché » et non sur ses concurrents américains actuels. La puissance commerciale de Microsoft se traduit par des revenus élevés provenant du secteur public. En Allemagne, rien qu'au niveau fédéral (c'est-à-dire sans compter les chiffres des 16 Länder et des plus de 11 000 communes), les coûts de licence versés à Microsoft s'élèvent à 197,7 millions d'euros. Et la tendance est à la hausse : depuis 2017, les coûts au niveau fédéral

ont augmenté de plus de 250 %, comme [le rapporte le magazine informatique heise](#). Sur le coût total, 98,5 millions d'euros sont consacrés à des licences à durée indéterminée, 29 millions à des modèles d'abonnement et 69 millions à « d'autres services et produits ».

Une [petite question posée au Bundestag allemand au début de l'année 2025 a révélé](#) que 99,9 % des dépenses d'exploitation pour les applications cloud de l'État fédéral concernaient des logiciels propriétaires. Microsoft détient ici la part la plus importante. Mais bien que le débat sur la politique numérique soulève de nombreux doutes et critiques quant à l'utilisation judicieuse et conforme à la loi des logiciels Microsoft et que de nombreuses questions ne soient pas encore définitivement clarifiées (voir X. ci-dessous), de nombreux organismes publics sont déjà en train de passer à Microsoft Teams et pourront alors discuter, travailler sur des documents et organiser des vidéoconférences via les serveurs accompagnés de licences ou d'abonnements Microsoft.

Mais est-il politiquement judicieux que l'État, client phare, dépende des décisions stratégiques d'un seul fournisseur ? Dans les sections suivantes, nous présentons quelques-unes des raisons pour lesquelles l'administration allemande est devenue si dépendante d'un seul fournisseur.

1. Les effets de plate-forme et de verrouillage favorisent une position dominante sur le marché

Le fait que Microsoft soit si largement répandu sur les ordinateurs de l'administration allemande ne s'explique pas uniquement par l'absence d'alternatives à Microsoft sur le marché ou par la qualité imbattable des produits « MS ». Microsoft a plutôt stratégiquement exploité, dans le développement de ses produits, depuis le système d'exploitation (Windows) jusqu'aux serveurs de messagerie électronique (Exchange) et désormais au cloud (Azure / OneDrive), a toujours exploité stratégiquement

ses relations politiques et administratives, qu'il a établies et entretenues depuis des décennies grâce à des activités de lobbying et à un travail de relations publiques important, ainsi que sa connaissance du marché et sa gestion des licences, afin de continuer à accroître sa part de marché dans le secteur public. On ne peut guère reprocher à l'entreprise elle-même son succès commercial : le groupe s'efforce d'améliorer son chiffre d'affaires et ses bénéfices et de commercialiser ses produits. Cela est légitime et son succès commercial mérite d'être reconnu.

Cependant, dans son rôle de pénétration du marché, Microsoft utilise des moyens qui tendent à compromettre l'objectif d'une concurrence loyale sur le marché intérieur de l'UE. La littérature économique parle d'*effets de verrouillage* : si le passage à un autre fournisseur est délibérément rendu si complexe par des circonstances factuelles que les organisations renoncent à changer de concurrent, le principe de l'offre et de la demande échoue. Si les responsables craignent qu'un changement coûte énormément de temps et d'argent, qu'il s'accompagne de changements internes importants et, dans le pire des cas, d'une perte de données, ils hésitent à franchir le pas, même si cela semble évident d'un point de vue économique ou qualitatif. *Ruppert Podszun*, professeur de droit de la concurrence, décrit les effets de verrouillage dans un chapitre de son livre **comme suit** : « En raison d'écosystèmes intégrés et fermés, les utilisateurs sont incités à ne pas quitter ces écosystèmes afin de profiter d'offres alternatives, pour autant qu'elles soient interopérables. » Grâce à sa stratégie de développement de produits dans un écosystème exclusif dominé par Microsoft, le groupe a réussi à tirer parti des effets de verrouillage à son avantage.

Microsoft utilise également sa position dominante sur le marché et sa marge de manœuvre financière pour façonner la chaîne d'approvisionnement selon ses propres idées.

Microsoft utilise également sa position dominante sur le marché et sa marge de manœuvre financière pour façonner la chaîne d'approvisionnement selon ses propres idées. Le groupe a réussi à plusieurs reprises à intégrer des concurrents européens dans son propre écosystème

en tant que partenaires commerciaux de Microsoft ou à les évincer de la concurrence par d'autres moyens. Le système d'octroi de licences et les canaux de distribution ont fait l'objet de critiques répétées. Dans le domaine du cloud computing, Microsoft aurait **délibérément poussé des fournisseurs indépendants d'infrastructures cloud à devenir des revendeurs de licences Microsoft**.

2. Never change a winning team – ou : seul celui qui a le libre choix est souverain.

Windows et Office étant déjà les leaders incontestés sur les ordinateurs des administrations, Microsoft souhaite également étendre ses parts de marché dans le domaine du cloud. Pour ce faire, le groupe tire parti de plusieurs avantages. Tout d'abord, le pouvoir de l'habitude au sein des administrations (« Nous avons toujours fait ainsi ») favorise un quasi-monopole (1.). De plus, Microsoft peut influencer l'offre et la demande grâce à sa politique d'entreprise en matière de développement des prix et des produits et à son réseau de distribution (2.). Comme Microsoft augmente continuellement **son chiffre d'affaires mondial** et a réalisé un bénéfice net de 72 milliards d'euros en 2024, le groupe utilise également sa marge de manœuvre financière pour mener des activités de marketing et de lobbying à grande échelle à Bruxelles et à Berlin (3.).

a) Le pouvoir de l'habitude dans l'administration publique et la pénurie de main-d'œuvre qualifiée

Ce n'est pas un cliché de dire que l'administration publique est soumise à des forces d'inertie particulièrement fortes. Quiconque souhaite abandonner l'environnement Outlook habituel ou supprimer Microsoft Word peut s'attendre à une forte résistance dans un premier temps. « Nous avons toujours fait cela avec Microsoft » peut rapidement devenir le cri de ralliement d'une opposition fondamentale qui étouffe dans l'œuf tout changement dans l'environnement de travail numérique. En coulisses, les décideurs politiques citent ces défis culturels administratifs comme la véritable raison de leur réticence politique à s'engager dans une ère post-Microsoft. Mais peut-être s'agit-il aussi d'une excuse commode. Une chose est sûre : lorsque le courage et l'énergie nécessaires à un projet d'une telle envergure font défaut au plus haut niveau politique, c'est généralement l'inertie de la masse (administrative) qui l'emporte.

Mais ce n'est pas seulement pour les utilisateurs du logiciel standard dans les administrations que l'abandon de l'écosystème Microsoft habituel peut entraîner des coûts supplémentaires considérables, c'est aussi le cas pour les services informatiques de l'administration. Le responsable informatique communal atteint rapidement ses limites lorsque les comptes de messagerie du centre de données administratif sont déjà configurés via Exchange et que le logiciel est mis à jour automatiquement, lorsque la gestion des licences avec les distributeurs Microsoft, qui s'efforcent d'entretenir la relation commerciale, est déjà bien rodée avec le service des marchés publics et lorsque de nombreux ordinateurs portables équipés de Windows et de la suite Office sont déjà en circulation. Car il est tout sauf facile de remplacer une infrastructure informatique complète, profondément marquée par les produits et applications Microsoft, par des alternatives, en particulier lorsque le service met également en œuvre des services OZG, exploite et entretient l'infrastructure informatique existante, traite les demandes d'assistance informatique du type « Pourquoi mon imprimante n'imprime-t-elle plus ? » et ne reçoit aucune aide ni incitation à la transition de la part des ministères compétents. À cela s'ajoute le fait que la pénurie de personnel informatique qualifié ne s'arrête pas aux portes de l'administration : les conditions de travail ne peuvent guère rivaliser avec celles de l'économie numérique, et les dirigeants des administrations s'intéressent souvent peu à la numérisation. Enfin, les écoles et les centres de formation professionnelle sont tellement habitués à Microsoft que la formation des informaticiens spécialisés se concentre sur la gamme de produits Microsoft et son intégration. Il manque donc non seulement le courage de changer, mais aussi les ressources humaines et les compétences nécessaires pour faire de grands progrès dans l'informatique administrative.

b) Quand le développement stratégique des produits et l'évolution dynamique des prix vont de pair...

L'annonce d'une décision stratégique au siège social de Redmond a mis de nombreux clients du secteur public sous pression : avec le passage à Microsoft 365, la direction de Microsoft souhaite qu'à partir de 2029 au plus tard, il ne soit plus possible d'utiliser les versions sur site des programmes Microsoft (par exemple Microsoft Office 2024) – une connexion à l'infrastructure cloud Azure

fournie par Microsoft sera obligatoire. Si l'administration publique souhaite continuer à utiliser l'environnement Office auquel elle est habituée, elle n'aura plus le choix à partir de 2029 : elle devra nécessairement s'intégrer encore plus profondément dans l'écosystème Microsoft et revoir son budget logiciel.

Une décision d'entreprise contraignante plutôt qu'une stratégie cloud réfléchie de l'administration

Bien que l'administration allemande n'ait jusqu'à présent pas montré une volonté très forte de passer à grande échelle au cloud computing, Microsoft tente désormais, avec l'annonce « à partir de 2029, uniquement un modèle d'abonnement », de la pousser vers une offre qui ne correspond pas forcément aux besoins réels des autorités. Le message de Redmond est clair : si les autorités souhaitent continuer à utiliser Outlook et Office, il est judicieux, compte tenu des campagnes marketing à l'ère du cloud, d'utiliser directement le « cloud public » comme

Les conséquences d'une dépendance de fait vis-à-vis de Microsoft sont particulièrement évidentes à ce stade.

nouveau support de stockage et plaque tournante des données pour l'administration publique. Les conséquences d'une dépendance de fait vis-à-vis de Microsoft sont particulièrement évidentes à ce stade. Au lieu de commencer par définir sa propre stratégie cloud et d'analyser quand un service cloud peut être utilisé de manière judicieuse dans le flux de travail de l'administration, puis de rechercher les fournisseurs appropriés, l'État se laisse entraîner par les décisions commerciales de Microsoft de passer entièrement au cloud. L'autodétermination et la liberté de choix stratégique concernant la propre infrastructure informatique de l'État sont tout autres.

L'abandon annoncé du modèle de licence aura également des répercussions prévisibles sur le principal moyen par lequel l'administration allemande obtient des licences Microsoft à des conditions spéciales : le contrat-cadre entre Microsoft et le ministère fédéral de l'Intérieur (BMI). Il constitue la base juridique pour l'achat de licences logicielles par les autorités et les organismes publics allemands. Non seulement les autorités fédérales, mais aussi les Länder, les communes et d'autres collecti-

vités peuvent invoquer les conditions préférentielles qui y sont prévues lorsqu'elles acquièrent des licences Microsoft. Elles peuvent faire des **contrats dits « contrats de conditions »** l'objet de leur procédure d'attribution. Par l'intermédiaire des **« Licensing Solution Partner » (LSP) du groupe Microsoft**, parmi lesquels Bechtle ou SoftwareONE, les villes et les autorités régionales achètent ensuite des licences Microsoft pour des logiciels standard et des environnements serveurs. Tous les trois ans, Microsoft et le BMI négocient de nouvelles conditions pour des objets de licence en constante augmentation. La prochaine période de trois ans n'a commencé qu'au printemps 2025. L'annonce par Microsoft de la fin progressive de son offre sur site d'interferait non seulement avec la structure et la nature juridique du contrat-cadre du BMI. Pour les renégociations prévues d'ici 2028, il faudra clarifier comment le « contrat Select Plus » devra être adapté compte tenu des futurs modèles d'abonnement. Dans le même temps, le gouvernement fédéral doit se demander s'il doit réellement prolonger ses relations contractuelles actuelles avec Microsoft, compte tenu de l'augmentation constante des engagements et des dépendances.

Prix, prix, prix – où cela va-t-il nous mener ?

Microsoft a mis en place un levier puissant avec la tarification de son cloud, car le passage à cette technologie permet au groupe de proposer dans un premier temps des prix très avantageux à ses clients existants afin d'inciter l'administration publique à effectuer une transition rapide et facile, puis d'augmenter progressivement les prix par la suite. Cela n'aurait rien d'étonnant : sur le marché privé des solutions cloud, une augmentation des prix de 11 % au 1er avril 2023 a suscité de vives critiques en Allemagne et en Europe. Certains concurrents ont déclaré que ces **augmentations de prix « frisaient le chantage »**. Depuis septembre 2024, **l'Office fédéral allemand des cartels observe** également de près la politique tarifaire du groupe et **soumet Microsoft à ce qu'on appelle une « surveillance étendue des abus » (§19a GWB)**. Microsoft avait également invoqué auprès des clients privés que les prix devaient refléter les fluctuations du cours du dollar américain et qu'ils seraient donc régulièrement ajustés à l'avenir. Une crise monétaire aux États-Unis ou une modification des conditions d'importation pourrait alors conduire le fisc allemand à être confronté d'un seul coup à une croissance exponentielle

des budgets informatiques, qui étaient en réalité prévus pour le développement de la numérisation administrative et la promotion de solutions cloud souveraines.

De plus, si un outil de communication (Microsoft Teams) ou une application cloud (OneDrive) est fourni directement – à première vue gratuitement – à un utilisateur privé ou public du système d'exploitation Windows ou de la suite Office, cela nuit à la concurrence libre et loyale, en particulier lorsque d'autres solutions ne sont pas du tout interopérables avec l'écosystème Microsoft. Au lieu de mettre en place une messagerie instantanée respectueuse de la protection des données pour les employés des administrations, qui soit si possible interopérable et garantisse ainsi le plus haut niveau possible de portabilité des données au sens du RGPD, une administration utilise alors gratuitement ou moyennant un léger supplément Microsoft Teams, qui n'offre justement pas ces fonctionnalités. L'autorité européenne de la concurrence **voit d'un œil critique ce type de modèles commerciaux**. En effet, pour diverses raisons, il peut sembler évident pour les services informatiques des administrations d'utiliser Teams pour la communication interne, car les serveurs et les ordinateurs portables sont de toute façon programmés pour Microsoft. La prochaine mise à jour du produit du fabricant intégrera et déploiera directement une nouvelle plateforme de communication. Cette approche stratégique a conduit l'administration à s'enfermer dans une cage dorée dont elle ne peut plus sortir facilement. Cette évolution se poursuit actuellement avec l'utilisation de l'intelligence artificielle, également issue du cloud.

c) Efforts considérables en matière de lobbying et de communication stratégique

La part de marché élevée des produits Microsoft dans l'administration publique n'est pas le fruit du hasard, mais résulte au moins en partie du travail intensif de lobbying et de relations publiques mené par le groupe Microsoft. **Selon Lobbypedia**, Microsoft dispose à Bruxelles « de son propre bureau de lobbying avec 17 lobbyistes (10 équivalents temps plein) », ce qui en ferait « la plus grande équipe de lobbying parmi les groupes technologiques en Europe ». Au cours de l'exercice 2019, le groupe a déclaré avoir dépensé « entre 5 000 000 et 5 250 000 euros » pour des activités de lobbying. **Selon statista**, Microsoft a déjà investi sept millions d'euros dans la communication politique au cours de l'exercice

2023. À titre de comparaison, Deutsche Telekom a dépensé 1,75 million d'euros et seule Meta Platforms Ireland Limited a dépensé plus, avec 9 millions d'euros. Le travail de relations publiques ne se limite pas aux lobbyistes internes à l'entreprise. Selon Lobbycontrol, Microsoft est membre ou sponsor de plusieurs groupes de réflexion, groupes de travail et associations professionnelles, de Digital Europe au Centre on Regulation in Europe (CERRE) en passant par l'European Internet Forum et l'European Policy Centre (EPC). À cela s'ajoute un réseau d'agences de communication politique, de publicité, de conseil politique et de grands cabinets d'avocats internationaux.

En Allemagne, il n'existe pas de chiffres fiables sur les dépenses de lobbying de Microsoft. Dans le registre des lobbyistes du Bundestag allemand, neuf personnes sont inscrites pour Microsoft Deutschland GmbH comme « représentant directement les intérêts » ; l'entreprise est également membre de 50 associations. Microsoft Deutschland GmbH est également partenaire de l'association professionnelle BITKOM et membre de l'Association fédérale de l'économie numérique (BVDW), qui représentent régulièrement les intérêts de l'économie numérique dans les procédures législatives et les audiences publiques.

En combinaison avec la stratégie globale du groupe, ses plus de 3 000 employés en Allemagne et 221 000 personnes dans le monde, le groupe Microsoft dispose d'un vaste réseau pour défendre ses propres intérêts commerciaux auprès des milieux politiques, de l'administration et de la société. La forte influence des grandes entreprises technologiques lors du processus législatif pour les nouvelles lois numériques de l'UE a souvent donné lieu à des reportages critiques, Microsoft étant souvent le fer de lance de la communication.

II. Propriétaire, peu sûr, illégal ? – Critiques à l'égard de l'utilisation de Microsoft dans l'administration

Les critiques à l'égard de la dépendance à grande échelle de l'administration allemande vis-à-vis des produits Microsoft se déclinent sous différentes facettes. Nous résumons ci-dessous les points essentiels.

1. Absence de contrôle sur le fonctionnement et la sécurité des logiciels

De nombreux organismes publics s'appuient principalement sur Microsoft pour leurs achats informatiques, car dans un environnement numérique déjà dominé par les produits Microsoft, il est facile et pratique d'acheter d'autres produits prêts à l'emploi auprès d'un seul et même fournisseur. Face aux start-ups GovTech, à une communauté de développeurs et d'entreprises open source, aux prestataires informatiques publics de l'État fédéral et des Länder ou aux consortiums de PME européennes, les responsables politiques ne croient souvent pas en leur capacité à développer l'infrastructure informatique allemande de manière sûre, fonctionnelle et fiable pour les années à venir, ni à la sécuriser et à l'exploiter à un niveau élevé. La dépendance vis-à-vis de Microsoft est également pratique : tout ce qui a déjà été externalisé ou acheté à Microsoft en matière d'infrastructure informatique devrait alors être réorganisé par l'État lui-même ou réparti entre de nouveaux acteurs. Les décideurs politiques craignent de ne pas disposer de la marge de manœuvre financière et des ressources humaines nécessaires pour passer à des alternatives propres ou plus coûteuses à exploiter. Et tout ministre ou secrétaire d'État qui échouerait dans un tel projet mettrait non seulement en péril sa propre réputation politique, mais aussi, dans le pire des cas, le bon fonctionnement de l'administration si les systèmes informatiques s'avéraient peu sûrs ou peu fiables.

L'achat de licences et d'abonnements auprès d'un acteur dominant sur le marché a toutefois pour effet secondaire que l'État n'est pas en mesure de contrôler le fonctionnement du logiciel ni d'en garantir la sécurité par ses propres moyens, car il ne dispose d'aucun pouvoir de négociation, ou d'un pouvoir insuffisant, et donc d'aucune influence sur le contenu, en raison de la position monopolistique du groupe.

L'achat de licences et d'abonnements auprès d'un acteur dominant sur le marché a toutefois pour effet secondaire que l'État n'est pas en mesure de contrôler le fonctionnement du logiciel ni d'en garantir la sécurité.

té par ses propres moyens, car il ne dispose d'aucun pouvoir de négociation, ou d'un pouvoir insuffisant, et donc d'aucune influence sur le contenu, en raison de la position monopolistique du groupe. L'une des principales raisons à cela est que Microsoft classe le code et les interfaces système comme secrets commerciaux. Le modèle commercial du groupe consiste à distribuer des logiciels dits « propriétaires » via des licences. Lorsque l'État allemand base ses processus de travail numériques sur les produits Microsoft, il ne reçoit qu'un fichier d'installation avec une clé de licence et, le cas échéant, une assistance, mais n'a pas accès au code source, conformément à la politique du « à prendre ou à laisser ». En raison des obligations liées à la licence, il n'a également aucun moyen d'adapter les produits de base à ses propres besoins. L'écosystème Microsoft étant délibérément fermé, c'est-à-dire que les normes et les interfaces ne sont pas conçues pour intégrer des produits concurrents, l'État ne peut construire son environnement informatique que de manière modulaire et limitée. Le logiciel étant propriétaire, les mises à jour le sont également. L'État ne peut pas vérifier ce qui est déployé en détail sur les ordinateurs et les serveurs de l'administration allemande lorsque Microsoft envoie une mise à jour de produit ou de sécurité. Les adaptations des produits sont effectuées à l'échelle mondiale, dans les foyers privés et les grandes entreprises, et ne sont, au mieux, que marginalement orientées vers les besoins des autorités allemandes. Lorsque des mises à jour sont déployées, l'État ne peut pas vérifier de manière fiable par ses propres moyens si le code comporte des failles de sécurité ou des portes dérobées qui rendent l'infrastructure informatique vulnérable. Cepen-

L'Allemagne n'ayant pas de poids dans les négociations, elle n'a aucune influence sur la politique de mise à jour et le développement des produits de Microsoft, ce qui réduit considérablement son influence sur son propre environnement de travail numérique.

dant, renoncer à renouveler régulièrement les applications logicielles pour cette raison ne serait pas non plus une bonne idée. En effet, sans mises à jour, les produits deviennent de moins en moins sûrs, notamment parce

que les failles de sécurité déjà connues (appelées « n-days ») restent ouvertes et que les systèmes sont ainsi largement exposés à d'éventuelles attaques. L'Allemagne n'ayant pas de poids dans les négociations, elle n'a aucune influence sur la politique de mise à jour et le développement des produits de Microsoft, ce qui réduit considérablement son influence sur son propre environnement de travail numérique.

2. Sécurité informatique et incidents de cybersécurité

L'une des conséquences de l'intégration profonde de l'administration dans l'écosystème Microsoft est que l'État allemand n'a plus le contrôle sur la sécurité permanente des bases de données publiques stockées sur les serveurs Microsoft, qu'il s'agisse d'un accès par des pirates informatiques (étrangers) ou par les services de renseignement américains. Si Microsoft ne se contentait pas de proposer des applications logicielles individuelles, mais que l'administration allemande devait gérer une grande partie de ses processus de travail numériques via un environnement cloud Microsoft complet, cela créerait également davantage de points d'attaque pour l'exécutif.

Plusieurs incidents de sécurité graves survenus récemment ont montré que la fidélité à l'écosystème Microsoft ne s'explique plus par le fait que le groupe est pour ainsi dire le seul garant de la sécurité informatique dans les organisations complexes. Le fait que l'une des clés principales utilisées pour le cryptage du cloud Azure ait atterri en Chine a notamment fait les gros titres. **Selon le BSI**, cela a permis au groupe de hackers Storm-0558 « d'accéder aux comptes de messagerie électronique de 22 organisations et institutions gouvernementales, principalement aux États-Unis, mais pas en Allemagne () (...). » On suppose toutefois que la clé aurait également pu être utilisée pour accéder à d'autres services cloud de Microsoft. Dans un rapport d'enquête, l'Agence américaine pour la cybersécurité et la sécurité des infrastructures (CISA) a reproché à Microsoft « de multiples défaillances en matière de cybersécurité », comme l'a rapporté [heise.de](https://www.heise.de).

Le groupe Microsoft a certes reconnu qu'il avait des lacunes en matière de sécurité informatique et a conclu des partenariats stratégiques avec des entreprises internationales de sécurité informatique ou les a rachetées. L'expert en sécurité informatique *Sandro Gaycken*

a déclaré **à la chaîne de télévision rbb** que les grands groupes numériques « ont racheté des entreprises de cybersécurité, les ont consolidées et intégrées à leurs produits ». Grâce à son intégration chez Microsoft, l'entreprise CrowdStrike « a obtenu une part de marché de 14 % », selon M. Gaycken. Mais ce partenariat avec CrowdStrike s'est retourné contre Microsoft en 2024. Une mise à jour de sécurité de CrowdStrike pour les applications Microsoft contenait un code erroné. En conséquence, des systèmes sont tombés en panne et des systèmes sensibles ont été exposés aux attaques. **Selon le groupe**, 8,5 millions d'appareils Windows ont été touchés dans le monde entier, dont, **selon le BSI**, des opérateurs d'infrastructures critiques en Allemagne. **L'opposition au Bundestag** est même allée jusqu'à qualifier Microsoft de « risque pour la sécurité nationale » en raison de la lenteur de l'enquête.

En cette période de turbulences géopolitiques, où le monde est de plus en plus en proie à une guerre hybride et à des conflits commerciaux qui s'intensifient, il faut s'attendre à ce que les attaques contre les infrastructures sensibles augmentent plutôt qu'elles ne diminuent à l'avenir. Chaque cyberattaque et chaque vulnérabilité chez Microsoft peuvent alors avoir des répercussions immédiates sur l'administration allemande lorsqu'elle utilise son infrastructure numérique. **Dans ce contexte**, l'expert en sécurité informatique **Sandro Gaycken ne voit qu'une seule solution** : « Il faut réduire la dépendance vis-à-vis de ces leaders très puissants du marché. » Mais il ajoute en même temps, à titre d'avertissement, qu'il faut prendre « un risque très important » et veiller à ne pas « aggraver la situation » en optant pour « des solutions moins chères ».

3. Questions en suspens concernant la protection des données lors de l'utilisation de Microsoft 365

Lorsque l'administration publique traite les données à caractère personnel des citoyens et de ses propres agents, elle est directement soumise au droit fondamental à l'autodétermination informationnelle et au droit fondamental à la protection des données. Le règlement général sur la protection des données de l'UE a pour objectif de « garantir un niveau élevé de protection des données » (considérant 6, phrase 5 du RGPD) et de préserver « les droits et libertés fondamentaux » des citoyens, « en particulier leur droit à la protection des données à caractère personnel, quelle

que soit leur nationalité ou leur lieu de résidence » (considérant 2, phrase 1 du RGPD). Si l'administration utilise les applications logicielles d'une entreprise pour accomplir ses missions publiques, ces programmes doivent également être conformes aux exigences en matière de protection des données. Étant donné que les logiciels Microsoft sont développés aux États-Unis et que certains d'entre eux étaient déjà disponibles sur le marché avant l'entrée en vigueur du RGPD, cela soulève des questions juridiques complexes. Au lieu de créer un nouvel environnement de travail numérique pour l'administration selon le principe « Privacy by Design » (art. 25 RGPD), les analyses en matière de protection des données portent donc souvent sur les fonctions des produits Microsoft qui sont compatibles avec les exigences en matière de protection des données – et celles qui ne le sont pas. Selon la devise : ce qui ne convient pas sera adapté. Cela résulte également en fin de compte de l'absence de parité de négociation de l'État allemand : lorsqu'un fournisseur détient le monopole sur les logiciels et les produits cloud, il devient de plus en plus difficile d'imposer ses propres conditions en matière de protection des données et de les contrôler efficacement.

Ce dilemme entraîne diverses incertitudes juridiques : la question de savoir si l'utilisation de l'application cloud Microsoft365 dans l'administration est compatible avec le RGPD divise depuis toujours. De nombreux défenseurs de la protection des données, dont la **Conférence sur la protection des données (DSK) des autorités de contrôle allemandes**, estiment que les applications Microsoft365 ne peuvent généralement pas être utilisées dans le respect de la protection des données. En novembre 2022, la DSK est parvenue à la conclusion suivante : « Tant que la transparence nécessaire concernant le traitement des données à caractère personnel issues du traitement des commandes à des fins propres à Microsoft n'est pas établie et que leur légalité n'est pas prouvée, cette preuve ne peut être apportée. » Outre le manque de transparence concernant les fonctions et les flux de données de l'application, les critiques portent également sur les transferts de données non traçables et la collecte extensive de données de diagnostic par Microsoft « en arrière-plan ».

En juillet 2025, **après une longue procédure d'examen** concernant l'utilisation de Microsoft365 par la Commission européenne, **le Contrôleur européen de la**

protection des données est parvenu à une conclusion différente. Selon lui, après de nombreuses adaptations techniques et juridiques, rien ne s'oppose plus à l'utilisation de Microsoft365. Le Contrôleur européen de la protection des données a fait valoir que « les mesures contractuelles, techniques et organisationnelles supplémentaires qui ont été mises en œuvre ou sont prévues en collaboration avec Microsoft » avaient dissipé les préoccupations en matière de protection des données. Il est convaincu que des analyses détaillées de l'environnement logiciel de Microsoft365 permettent de formuler les conditions d'adaptation du produit qui rendraient Microsoft365 conforme au RGPD. Cependant, les documents et assurances précis fournis par Microsoft dans le cadre de la procédure ne sont pas accessibles au public. On ne sait pas non plus si d'autres autorités de contrôle, voire des tribunaux, se rallieront à cette évaluation. En fin de compte, la décision du Contrôleur européen de la protection des données n'améliore pas la protection des données par la négociation équitable des conditions-cadres pour l'utilisation du cloud, mais se contente de patauger dans les problèmes sans en résoudre la cause réelle, qui réside entre autres dans la position monopolistique de l'entreprise – conséquence de décennies de dépendance vis-à-vis d'un seul fournisseur.

Chapitre 3 :

L'informatique ne peut pas vivre – avec ou sans Microsoft ? Un cloud « souverain », s'il vous plaît !

Une administration publique numérisée sans Microsoft, cela n'existe pas actuellement. Ni en Allemagne, ni à l'échelle internationale. Personne n'a encore rattrapé l'avance prise par Bill Gates avec son empire dans le domaine de l'informatique domestique et professionnelle, et même à l'ère du cloud, cela ne semble pas près de changer. Seule la Chine semble pouvoir s'appuyer sur des solutions nationales sur le marché du cloud avec *Alibaba Cloud* et *Tencent Cloud*.

Mais la dépendance de l'administration allemande à l'égard de Windows, Office et Teams est-elle gravée dans le marbre ?

Une chose est sûre : dans un monde idéal, l'État allemand ne dépendrait pas de fournisseurs individuels et pourrait composer l'offre qui lui convient à partir du portefeuille de produits de différents fournisseurs informatiques. Un ordinateur portable d'ici, un système d'exploitation de là, un environnement Office d'ailleurs et un serveur de messagerie d'un autre endroit – et tout cela pourrait être interconnecté de manière interoperable et remplacé de manière modulaire. Les interfaces ouvertes seraient la norme. En tant que client de référence, l'État pourrait commander des solutions sûres et faciles à utiliser, et les faire personnaliser de manière à ce qu'elles répondent aux besoins réglementaires et orientés vers l'utilisateur de l'administration. Il y aurait des infrastructures multi-cloud et des obligations open source claires dans les conditions d'attribution des marchés. Il ne ferait aucun doute que les données publiques ne peuvent être transférées vers des pays tiers ou que l'environnement logiciel ne peut être contrôlé à distance depuis un autre continent, voire désactivé.

Mais la réalité est la suivante : les autorités allemandes se sont profondément engagées dans l'écosystème Mi-

crosoft et continuent de dépendre des logiciels du groupe pour leur travail quotidien. Un changement précipité, du jour au lendemain pour ainsi dire, n'est donc guère réaliste. Mais même les initiatives individuelles de certains Länder peuvent se révéler sans issue si personne ne les suit à long terme. En effet, tous les acteurs devraient en réalité s'associer pour initier un changement d'une telle ampleur, définir ensemble les meilleures conditions, les exiger contractuellement, faire pression pour obtenir des prix avantageux et établir des interfaces communes pour l'échange au sein de l'État fédéral. Mais pourquoi cela ne se produit-il pas ?

Dans les années 1990, il existait deux géants dans le domaine de l'équipement bureautique numérique : Microsoft et Apple. Ils ont construit deux empires concurrents sur la base de systèmes d'exploitation qui, jusqu'à

L'administration allemande étant soumise à l'impératif de rentabilité, les postes de travail PC moins coûteux équipés de Microsoft Windows et Microsoft Office se sont imposés comme la norme dans les bureaux administratifs.

aujourd'hui, sont difficilement interoperables. L'administration allemande étant soumise à l'impératif de rentabilité, les postes de travail PC moins coûteux équipés de Microsoft Windows et Microsoft Office se sont imposés comme la norme dans les bureaux administratifs. C'est ainsi qu'a commencé l'ère des licences logicielles. Dans la pratique, cela se passait généralement ainsi : Microsoft accordait des licences pour ses produits, soit directement, soit par l'intermédiaire de sociétés tierces, établissant ainsi des relations économiques et des chaînes d'approvisionnement avec presque toutes les autorités

allemandes qui souhaitent s'équiper numériquement. Le réseau de distribution stratégique, alias l'écosystème Microsoft, s'est rapidement imposé et domine encore aujourd'hui les décisions des services d'attribution des marchés publics municipaux et nationaux. Le domaine connexe de l'approvisionnement informatique s'est développé parallèlement à la transformation numérique au fil des ans sur les plans juridique, organisationnel et stratégique.

À plusieurs reprises, des stratégies politiques, parfois à grande échelle, ont été mises en place pour se libérer des dépendances existantes et entrer de manière souveraine dans l'ère du cloud. Le domaine du cloud computing regorge actuellement d'idées et d'approches stratégiques :

- de la **consolidation informatique au niveau fédéral**,
- en passant par les stratégies multicloud telles que le « **Deutsche Verwaltungscld** » (cloud administratif allemand)
- ou le « **Sovereign Cloud Stack** ».
- Initiatives dans le domaine du « **cloud computing** » **au niveau de l'UE**
- La « **Semaine de l'open source** » au niveau de l'ONU en 2025

Mais entre les documents stratégiques, les tableaux d'affichage, les cartes mentales et les belles présentations PowerPoint, et un changement de cap dans la salle des machines numérique de l'administration, le chemin est encore long. Sans leadership politique, c'est-à-dire sans la force nécessaire pour s'imposer « d'en haut » malgré les résistances internes et externes, et sans une connaissance approfondie de l'écosystème existant et des alternatives possibles, un projet informatique d'une telle envergure ne peut aboutir.

Les structures fédérales en Allemagne rendent encore plus difficile la recherche d'un consensus politique pour explorer de nouvelles voies, mettre en place une informatique administrative ouverte et modulaire et abandonner les dépendances existantes. En effet, les Länder et les communes sont en principe libres de choisir comment ils équiperont leurs administrations en personnel et en matériel technique. Il en résulte que chacun fait plus ou moins cavalier seul : certaines administrations **travaillent déjà avec Microsoft365** et communiquent en interne via

MS Teams ; d'autres utilisent des solutions de visioconférence et de messagerie ouvertes, mais exploitent leurs serveurs de messagerie avec MS Exchange ; d'autres encore en sont encore au stade des licences sur site d'Outlook, Word, Powerpoint et autres, sans connexion au cloud. Parallèlement, Microsoft, SAP et d'autres proposent le « **Delos Cloud** », qui permet d'utiliser Microsoft365 dans un cloud qui n'est pas hébergé sur les serveurs Microsoft, mais chez une filiale de SAP (nous y reviendrons dans un instant).

Et lorsque le partenaire commercial éprouvé de Microsoft passe au service informatique et vante les nouvelles possibilités, certains responsables administratifs sont tentés d'acheter les « innovations » nécessaires directement auprès de Microsoft. La pandémie de coronavirus a encore accentué cette tendance. Avec les restrictions de contact et la fermeture des administrations, une chose était claire : l'administration doit rester opérationnelle, et pour cela, elle doit communiquer numériquement, partager des données et rester connectée à l'infrastructure existante. Pour de nombreux décideurs, miser sur Microsoft était la solution la plus sûre et la plus rapide. Une fois de plus, des faits ont été créés qui, maintenant que Microsoft365 ou Teams sont « déjà là », ne peuvent plus être facilement annulés.

En conséquence, la liberté de choix des utilisateurs européens est considérablement réduite par des tactiques ciblées de licence et de regroupement, un lobbying constant et des modèles commerciaux qui ont acquis une position dominante sur le marché grâce à des effets de verrouillage et de plateforme. Certes, des groupes informatiques alternatifs collaborent déjà dans le cadre de procédures d'attribution de marchés publics afin de briser cette monopolisation dans le secteur du cloud, mais il n'est pas encore certain que les entreprises soient prêtes à unir leurs forces de leur propre initiative. En juin 2025, **Reuters a annoncé** que Telekom, IONOS et Schwarz ne souhaitent pas se présenter en tant que consortium commun pour les nouveaux programmes de l'UE. Une procédure intelligemment conçue et coordonnée au niveau fédéral pour développer et exploiter une alternative ouverte à Microsoft Office et à l'environnement cloud de Microsoft au sein d'un consortium pourrait toutefois donner naissance à la plateforme de travail numérique de l'administration publique du futur dans un écosystème numérique ouvert, libre et fonctionnel.

Chapitre 4 :

Adaptations de produits et offres de Microsoft entre efforts sérieux et « sovereignty washing »

Afin de répondre aux critiques formulées à l'encontre de son modèle commercial en matière de protection des données, de politique numérique et de droit de la concurrence, et de convaincre les décideurs politiques que les produits Microsoft restent le meilleur choix pour l'administration allemande, le groupe a procédé ou proposé diverses adaptations de ses produits.

I. Programme européen de sécurité

En juin 2025, Microsoft a **annoncé un « programme européen de sécurité »**. Dans le cadre de ce programme, Microsoft souhaite partager davantage d'informations sur les menaces basées sur l'IA avec les gouvernements et fournir en temps réel des données relatives à la sécurité, générées notamment à la suite des cyberattaques continues contre l'écosystème Microsoft. Grâce à ce programme, le groupe souhaite investir dans les capacités locales en matière de cybersécurité et dans la résilience numérique des États, des autorités et de la société civile. De nouveaux partenariats avec les autorités répressives et des organisations telles qu'Europol doivent permettre de lutter plus efficacement contre les cybercriminels et les attaques orchestrées par des États. Microsoft souhaite détecter plus rapidement les infrastructures malveillantes et les scénarios d'attaque et les désactiver automatiquement.

Compte tenu de la menace hybride qui pèse sur le cyberspace, soulignée depuis de nombreuses années par le BSI, les services de renseignement et les responsables politiques en matière de sécurité, il est tout à fait judicieux que Microsoft utilise ses capacités de groupe international pour soutenir la sécurité des systèmes informatiques publics. Microsoft souhaite notamment offrir **une aide gratuite** contre les nouvelles formes de cyberattaques orchestrées et menées à l'aide de l'IA. Dans le même temps, le programme européen de sécurité ressemble quelque peu à une campagne de marketing. En effet, Mi-

crosoft avait fait les gros titres de manière plutôt négative ces dernières années en raison de plusieurs incidents de sécurité liés à CrowdStrike et à la clé principale du cloud Azure (voir ci-dessus). Aujourd'hui, en ces temps incertains, Microsoft propose soudainement son aide en tant que grand seigneur de l'informatique afin de protéger le continent européen dans un espace numérique en pleine tourmente.

II. Conditions de protection des données négociées individuellement

Les autorités chargées de la protection des données au niveau national et européen ont toujours critiqué l'utilisation des produits Microsoft, en particulier Microsoft365 basé sur le cloud, en raison du manque de transparence et de contrôle des flux de données dans la salle des machines de Microsoft (voir ci-dessus). En tant que groupe international, Microsoft a également dû relever le défi de formuler des conditions de protection des données sur mesure et suffisantes pour chaque région du monde et chaque environnement réglementaire, et d'adapter techniquement sa gamme de produits.

Lorsque les organisations achètent des logiciels standard, elles n'ont souvent pas la possibilité de négocier individuellement les conditions avec les grandes entreprises internationales, mais doivent se contenter des conditions générales de protection des données en vigueur sur leur marché ou dans leur secteur. **Selon** le magazine **informatique** c't 2024, certains gouvernements régionaux ont désormais mis fin à cette dépendance vis-à-vis des clauses standard des conditions de protection des données, suite aux critiques **formulées** par le commissaire régional à la protection des données et à la liberté d'information (LfDI) et la DSK.

Le Land de Basse-Saxe a ainsi négocié des règles spéciales avec Microsoft. Microsoft s'est engagé à ne stocker

et traiter les données que sur des serveurs européens, tandis que l'assistance informatique ne proviendra que de pays permettant une collaboration « conforme au RGPD » avec Microsoft. Les flux de données provenant des serveurs de l'UE et le transfert de données vers les États-Unis à des fins d'« analyses de fond » ou d'assistance resteraient alors possibles conformément au contrat, mais leur ampleur serait réduite. Une partie des conditions individuelles pourrait également consister à ce que seules certaines catégories de données soient traitées et transmises à des fins d'assistance, comme la Commission européenne semble l'avoir négocié avec Microsoft. Mais même dans ce cas, la question de savoir si l'assurance et la pratique réelle sont vraiment compatibles resterait ouverte. Le problème du « Cloud Act » resterait également sans solution.

En outre, Microsoft supprime en Basse-Saxe certains services particulièrement opaques en arrière-plan, tels que les données de diagnostic et Teams Analytics. Là encore, la question reste ouverte de savoir si cela suffira à interdire efficacement les flux de données importants ou à les contrôler de manière suffisante, et comment l'administration réagirait si Microsoft augmentait considérablement ses prix ultérieurement ou désactivait ou limitait les licences ou les modèles d'abonnement.

En outre, les autorités souhaitent garantir, par le biais d'instructions de travail internes relatives à l'utilisation des produits Microsoft, que certaines données particulièrement sensibles, telles que les données sociales ou médicales, ne soient pas traitées et échangées via MS Teams. Étant donné que le facteur humain est souvent le maillon faible et qu'il est difficile de faire respecter et de contrôler à grande échelle de telles directives purement internes, il subsiste en tout état de cause une incertitude résiduelle non négligeable.

III. La solution Delos : faire exploiter les centres de données par des entreprises européennes – (seuls) les logiciels proviennent de Microsoft

Mais que se passerait-il si les produits Microsoft basés sur le cloud, tels que Microsoft 365, étaient fournis dans des centres de données protégés appartenant à des entreprises européennes, auxquels seuls les organismes publics sont connectés ? Cela garantirait en théorie

que le retour des données vers les États-Unis « en arrière-plan » soit complètement bloqué. Même si le gouvernement américain demandait à l'entreprise de fournir des données européennes, Microsoft ne serait en fait pas en mesure de le faire. En effet, le contrôle appartiendrait uniquement aux exploitants des centres de données.

Un consortium composé de Microsoft, SAP et Arvato s'est lancé dans la résolution du dilemme des transferts internationaux de données. Une autorité publique pourrait alors réserver des services cloud auprès de Microsoft via la société Delos GmbH, filiale d', contrôlée par le géant allemand de l'Internet SAP, et éviterait ainsi d'acheter directement des logiciels et des infrastructures au groupe Microsoft et de les faire fonctionner sur son infrastructure. Une solution similaire existe en France : Capgemini et Orange y ont fondé la coentreprise « Bleu ». La promesse de Bleu et Delos est la suivante : les centres de données et les données sont sous contrôle national, seules les mises à jour logicielles proviennent de Microsoft aux États-Unis. À première vue, la promesse de Delos, filiale de SAP, semble séduisante :

« Les services de la plateforme cloud souveraine comprennent notamment les outils de collaboration et les solutions de productivité complets de Microsoft Office 365. La plateforme cloud sera techniquement, opérationnellement et juridiquement souveraine, conformément aux exigences réglementaires du gouvernement fédéral. Delos Cloud est ainsi actuellement la seule offre cloud à satisfaire pleinement aux exigences du BSI en matière de sécurité informatique et de protection du secret, ainsi qu'aux exigences légales en matière de protection des données, en accord avec le commissaire fédéral à la protection des données et à la liberté d'information (BfDI). En tant que propriétaire de l'infrastructure, Delos Cloud GmbH prend en charge à la fois l'exploitation de la plateforme et la concession de licences pour ses produits. »

Un inconvénient de la structure de l'entreprise : les prix sont 15 % plus élevés que la variante « Microsoft pur » avec le cloud Microsoft courant, comme le rapporte Computerwoche. Le prix plus élevé est compréhensible d'un point de vue économique, car les clouds Delos impliquent bien plus qu'un simple achat de licence dans la

gamme de produits Microsoft courante. Du point de vue des différentes autorités régionales ou locales, le choix se poserait alors entre « Microsoft pur » via le contrat-cadre du BMI et la variante plus coûteuse « Delos » – mais au final, tous les chemins mèneraient à nouveau à Microsoft.

Reste à savoir si cette solution protège réellement contre les fuites de données vers les services de sécurité américains, les attaques de pirates informatiques dues à un manque de sécurité informatique ou le durcissement des mesures dans les conflits commerciaux avec l'administration Trump. Le directeur de Delos, Georges Welz, a déclaré **dans une interview accordée à heise** : « Comme le cloud est sous notre contrôle, personne ne peut directement en restreindre le fonctionnement. Et s'il n'y avait plus de mises à jour, nous pourrions continuer à travailler pendant des mois, car le cloud fonctionne également de manière autonome. À cet égard, nous offrons une véritable souveraineté, à savoir un délai d'action pour réagir. » Cela signifie déjà que, dans le pire des cas, le cloud Delos ne pourrait plus fonctionner à long terme. Cela mettrait de facto en danger le fonctionnement de l'ensemble de l'administration. La période de transition, que Welz estime à « plusieurs mois », pourrait en fait se réduire à 0 jour si, par exemple, on apprenait que la dernière mise à jour des systèmes – comme dans le cas de Crowdstrike (voir ci-dessus) – a entraîné une faille de sécurité.

Et indépendamment des arguments techniques susmentionnés, il faut également ajouter ici qu'une solution partiellement souveraine telle que Delos ne rendrait en aucun cas l'Allemagne plus indépendante dans ses décisions d'achat, car l'État, en tant que client principal, resterait lié au logiciel du groupe et à ses conditions de licence restrictives. Malgré le montage juridique mis en place par l'entreprise Delos pour faire appel à un intermédiaire allemand, tous les chemins techniques mèneraient finalement à Microsoft. En fin de compte, la solution peut donner l'impression d'une souveraineté numérique, mais en réalité, les anciennes dépendances persistent sous une nouvelle forme.

IV. Limite des données et instances locales

Pour répondre à la crainte que le gouvernement américain puisse accéder aux bases de données et au contenu

des communications de l'administration publique, Microsoft a annoncé trois mesures supplémentaires : une frontière des données, des gardiens des données et des instances exploitées localement.

D'une part, Microsoft souhaite introduire une « limite de données » dans ses processus de traitement complexes pour l'offre « Sovereign Public Cloud ». Sur le fond, cela correspond aux conditions de protection des données négociées individuellement par la Basse-Saxe, selon lesquelles toutes les données des clients ne sont traitées qu'au sein des frontières de l'UE. À cela s'ajoute une adaptation concernant le cryptage, un aspect important pour la sécurité des données : la clé principale (« clé de cryptage ») doit rester exclusivement chez le client.

Avec la mesure « Data Guardian », Microsoft s'engage à ce que l'accès administrateur aux services cloud européens ne soit plus exercé que par des employés de Microsoft résidant en Europe. Si, dans certains cas, par exemple pour des questions d'assistance complexes, un accès à distance depuis les États-Unis s'avère nécessaire, celui-ci ne sera possible qu'avec l'autorisation expresse des collègues européens et fera l'objet d'un enregistrement strict. De cette manière, les personnes situées en dehors de l'UE auront moins souvent accès à l'infrastructure cloud.

Selon Microsoft, « Microsoft 365 Local » permettra également à l'avenir d'utiliser l'environnement logiciel sans connexion fixe et permanente à l'environnement cloud de Microsoft.

Selon Microsoft, « Microsoft 365 Local » permettra également à l'avenir d'utiliser l'environnement logiciel sans connexion fixe et permanente à l'environnement cloud de Microsoft. L'exploitation d' r sur des infrastructures propres resterait ainsi possible si les autorités ne voyaient aucune raison d'utiliser une solution basée sur le cloud. S'agit-il finalement d'un revirement par rapport à l'annonce de ne plus proposer ni développer de logiciels sur site à partir de 2029, ou d'une intégration d'une variante Microsoft365 Local « pour les produits par abonnement ou cloud » quelque peu plus sécurisée, *qu'Andreas Thys* qualifie de « bizarre » **dans son article invité** ?

Même si, à l'avenir, le traitement des données devait se faire exclusivement au sein de l'UE sous la responsabilité de filiales européennes entièrement soumises au RGPD, la question reste ouverte de savoir dans quelle mesure de telles mesures rendent réellement « souveraine » l'administration publique à moyen et long terme. Du **point de vue d'Andreas Thyen**, les « contre-mesures présentées aujourd'hui – EU Data Boundary, Data Guardian, instances exploitées localement – (...) sont des mesures de relations publiques ciblées. On espère obtenir un contrôle maximal sans avoir à renoncer à la souveraineté technique ». Le directeur de recherche du cyberintelligence.institute, le professeur Dennis-Kenji Kipker, **arrive à la conclusion suivante** : « Les promesses en matière de sécurité sont construites sur du sable ». En effet, selon **M. Kipker dans un commentaire publié dans IT Daily**, à y regarder de plus près, il ne s'agit ni d'une véritable frontière des données, ni de la souveraineté de l'utilisateur sur ses propres données stockées dans le cloud de Microsoft. **Le professeur Harald Wehnes, porte-parole du groupe de travail « Souveraineté numérique » de la Gesellschaft für Informatik e. V. (société allemande d'informatique)**, s'exprime de manière encore plus dramatique : « Sous le couvert de la « souveraineté

« Sous le couvert de la « souveraineté numérique », les groupes technologiques poursuivent clairement l'objectif d'attirer l'Europe vers des solutions irréversibles et coûteuses.

numérique », les groupes technologiques poursuivent clairement l'objectif d'attirer l'Europe vers des solutions irréversibles et coûteuses. Celles-ci sont destinées à consolider leur pouvoir sur le marché et, au final, à leur permettre d'exercer un contrôle encore plus grand sur les données et les technologies. » Ces déclarations montrent clairement que, quelle que soit la voie choisie par Microsoft, les « mesures alternatives » proposées ne feront qu'accroître la dépendance et lier encore davantage les clients à un environnement fermé, à l'opposé de la souveraineté numérique. La domination sous-jacente de Microsoft et sa capacité à dicter ses conditions et à fidéliser ses clients par le biais de licences et d'autres moyens ne changent en rien avec ces propositions.

Chapitre 5 :

Résumé et recommandations d'action

Les produits Microsoft dominent l'environnement de travail de l'administration publique. Le leader du marché souhaite également conserver et développer ses parts de marché dans le secteur public sur le marché d'avenir du cloud computing. En effet, plus l'administration est interconnectée, plus il est important de ne pas traiter et stocker les documents uniquement dans des silos administratifs locaux, mais d'utiliser les systèmes informa-

En annonçant son intention de passer systématiquement à des modèles d'abonnement avec abonnement Azure obligatoire à partir de 2029, Microsoft a mis l'administration allemande sous pression.

tiques de manière collaborative et numérique au-delà des frontières administratives. En annonçant son intention de passer systématiquement à des modèles d'abonnement avec abonnement Azure obligatoire à partir de 2029, Microsoft a mis l'administration allemande sous pression. Dans le même temps, cela ouvre une fenêtre d'opportunité pour planifier stratégiquement et mettre en œuvre progressivement une transition vers un environnement de travail numérique ouvert, sûr et souverain pour l'administration publique. Les priorités politiques que sont la souveraineté numérique, la protection des données et la cybersécurité pourraient ainsi être mises en œuvre grâce à des solutions sur mesure, au lieu de rester confinées dans un écosystème fermé présentant des inconvénients stratégiques.

Comme Microsoft souhaite continuer à développer ses parts de marché dans le secteur public et consolider sa position dans le domaine du cloud computing, le groupe réagit avec toute sa puissance marketing aux critiques multiples et aux incidents de sécurité débattus publiquement. Sur la voie politiquement tracée vers un « cloud souverain » en Allemagne et en Europe, on

observe un jeu du chat et de la souris entre les critiques en matière de politique numérique et de protection des données et les annonces sans cesse renouvelées du groupe. Même si chacune des mesures tente de répondre à certaines critiques et vise à atténuer certains risques, la dépendance actuelle de l'administration allemande à l'égard de la gamme de produits Microsoft et le risque de perte de contrôle ou de fuites de données importantes persistent.

La collaboration étroite entre l'administration publique et Microsoft suscite régulièrement des critiques sur plusieurs aspects centraux : protection des données et transparence, sécurité des données et cybersécurité, ainsi que contrainte monopolistique du cloud au lieu d'une stratégie cloud indépendante. Les nombreuses propositions et adaptations de produits présentées par Microsoft ces dernières années ne répondent que partiellement ou de manière rudimentaire à ces quatre préoccupations centrales. C'est l'énorme domination du marché par un groupe international et son modèle commercial, caractérisé depuis des décennies par un comportement discutable en matière de concurrence, un écosystème fermé, un développement dynamique de concepts commerciaux et une politique de prix, qui font obstacle à l'objectif d'un environnement de travail souverain sur le plan numérique pour l'administration publique en Allemagne. Il est temps de procéder à une réorientation stratégique. Si l'on entend par « souveraineté numérique » essentiellement la liberté de choix et la possibilité de contrôler de manière indépendante l'infrastructure informatique publique et les flux de données administratives, seule une réorientation complète du paysage informatique public peut conduire à long terme à un objectif politique.

Le contrat-cadre conclu entre le ministère fédéral de l'Intérieur et Microsoft constitue le principal outil juridique et politique permettant de contrôler l'interdépendance concrète et la coopération contractuelle avec Microsoft.

Les conditions du contrat-cadre conclu au printemps 2025 ne pourront pas être modifiées **à court terme** au cours des trois prochaines années, mais ce temps peut être mis à profit pour se positionner et se préparer au mieux en vue d'une éventuelle prolongation en 2028 et pour initier **à long terme** une réorientation complète vers l'objectif de « souveraineté numérique » avec des logiciels ouverts et une stratégie multi-cloud souveraine.

Mesures à court terme jusqu'en 2028 :

- **Suivi des coûts d'acquisition informatique via le contrat-cadre BMI par le gouvernement fédéral**

Le gouvernement fédéral et la Conférence des ministres du numérique (DMK) devraient se faire une idée précise, et en informer le public, du montant total des dépenses fiscales engagées actuellement par l'État fédéral, les Länder et les communes pour les licences Microsoft. Outre une enquête systématique – aussi contraignante que possible – auprès des autorités fédérales, des Länder et des communes, les autorités fiscales pourraient également demander aux Licensing Solution Partner (LSP) de divulguer le chiffre d'affaires annuel qu'ils réalisent grâce au modèle commercial « achat de licences sur la base du contrat-cadre du BMI ». En effet, sans chiffres fiables, il est impossible de calculer et de planifier la marge de manœuvre financière nécessaire à un changement de stratégie.

- **Études de faisabilité et de potentiel visant à accroître la liberté de choix dans certains domaines de produits**

Sur la base du suivi des coûts globaux, le gouvernement fédéral allemand et DMK devraient examiner, dans le cadre d'études de faisabilité pour un marché du cloud ouvert, interopérable et équitable, plusieurs scénarios en faveur de la liberté de choix et de la souveraineté numérique, ainsi que leurs conditions-cadres politiques, juridiques et techniques. Une attention particulière devrait être accordée aux domaines de produits suivants : systèmes d'exploitation, logiciels de bureau, communication (e-mail et messagerie instantanée), collaboration (travail collaboratif sur des documents et stockage partagé de données) et services multi-cloud, afin de mettre fin à la dépendance actuelle à l'égard d'un seul fournisseur. L'étude économique et technique devrait prévoir,

sur la base des dépenses annuelles et de l'équipement informatique actuel, si des offres alternatives pourraient être stratégiquement acquises et mises en œuvre à l'avenir. Si des lacunes dans l'offre sont identifiées sur le marché, l'étude devrait également examiner comment le gouvernement fédéral et les Länder pourraient les combler de manière ciblée par le biais de la recherche et du soutien aux entreprises. L'analyse du potentiel devait également inclure des entretiens avec des entreprises de l'écosystème Microsoft, des concurrents européens, des pouvoirs adjudicateurs au niveau régional et local, ainsi que des associations de protection des consommateurs et des entreprises, afin d'examiner de plus près non seulement les chiffres, mais aussi la stratégie commerciale réelle.

- **Intensification des enquêtes en matière de droit de la concurrence sur l'écosystème Microsoft et l'octroi de licences dans le domaine de l'administration publique**

Dans le cadre de ses enquêtes au titre de l'article 19a de la loi allemande sur les ententes (GWB), l'Office fédéral allemand des ententes (Bundeskartellamt) devrait mettre en place un groupe de travail indépendant chargé d'examiner en détail le réseau de distribution du groupe Microsoft et l'utilisation des produits Microsoft dans l'administration publique. Le législateur budgétaire devrait fournir à l'autorité des ressources suffisantes pour enquêter sur les monopoles anticoncurrentiels et, le cas échéant, les démanteler. Une enquête à grande échelle, menée éventuellement en collaboration avec la Commission européenne et d'autres États membres, pourrait révéler dans quelle mesure la position dominante sur le marché est maintenue ou renforcée par les conditions contractuelles des contrats de licence, des contrats cloud et des contrats-cadres, mais aussi par l'influence et le contrôle de facto du groupe Microsoft et de ses partenaires commerciaux souvent exclusifs dans le domaine des marchés publics ou des procédures d'achat complexes. Toutes les pratiques commerciales qui entravent la concurrence loyale et la liberté de choix réelle, en particulier les pratiques restrictives en matière de licences, devraient être identifiées et empêchées par des mesures réglementaires appropriées.

- **Dialogues stratégiques sur le numérique avec des partenaires internationaux sur la question de la souveraineté numérique dans l'administration informatique**

Le gouvernement fédéral devrait mettre en place et promouvoir des formats de dialogue internationaux stratégiques dans lesquels la République fédérale d'Allemagne pourrait échanger de manière structurée avec la Commission européenne et d'autres États membres de l'UE (par exemple l'Italie, la France, les Pays-Bas, le Portugal et l'Estonie), mais aussi avec des partenaires stratégiques du monde entier (par exemple la Corée du Sud, le Japon, le Canada ou l'Australie) sur la voie vers une informatique administrative souveraine. Il devrait pour cela faire appel à la société civile, au monde scientifique, mais aussi aux entreprises européennes et à la communauté open source. L'étendue et la portée des dialogues stratégiques sur le numérique peuvent être envisagées et conçues de manière très différente : outre un échange institutionnalisé d'expériences à différents niveaux sur la collecte des meilleures pratiques dans le domaine des stratégies de souveraineté informatique, sur des projets de recherche communs ou même des contrats de développement transnationaux pour des solutions informatiques individuelles, jusqu'à la formation d'un groupe de négociation commun pour des contrats-cadres solides et uniformes avec Microsoft. Là où le groupe Microsoft a pu obtenir un avantage dans les négociations des contrats-cadres et des contrats de licence grâce à ses réseaux de distribution très denses et à ses cabinets d'avocats hautement qualifiés, les pouvoirs adjudicateurs publics doivent également tirer parti de cet avantage dans les négociations grâce à l'échange d'expériences et au transfert de connaissances.

Mesures à moyen terme pour les négociations du prochain contrat-cadre du BMI :

- **Liberté de choix « light » : possibilité de choisir entre les nouveaux et les anciens produits Microsoft**

Il est économiquement compréhensible que Microsoft souhaite passer de son modèle d'achat de licences à durée indéterminée à un modèle d'abonnement. Le groupe s'octroie ainsi une plus grande

marge de manœuvre sur le plan contractuel et peut empêcher plus efficacement l'utilisation abusive des licences. Du point de vue de l'administration publique, le passage à des solutions basées sur le cloud serait toutefois un pas de trop avant le deuxième. En particulier pour les logiciels standard utilisés au quotidien dans les bureaux, l'administration dispose déjà de licences logicielles et, dans de nombreux domaines, il n'y a pas de nécessité pratique urgente d'abandonner l'utilisation sur site d'Outlook, d'Office ou des messageries instantanées. Néanmoins, l'État devrait négocier avec assurance et mettre dans la balance l'option d'un changement stratégique vers des alternatives. Avec la suppression annoncée des solutions sur site à partir de 2029 et la nécessité qui en découle de passer obligatoirement au cloud Microsoft, cette question est déjà d'actualité et il est donc impératif de créer dès que possible les conditions juridiques et factuelles permettant une véritable liberté de choix sur le marché du cloud.

- **Ancrer contractuellement la transparence des coûts de licence à tous les niveaux**

Il est intolérable que Microsoft dispose de chiffres précis sur son volume d'affaires avec l'administration allemande, mais que le public doive régulièrement estimer le montant des deniers publics consacrés aux licences Microsoft. Lors des négociations sur un contrat-cadre, le gouvernement fédéral devrait insister sur la mise en place d'un instrument de suivi permettant de documenter de manière accessible et publique les dépenses annuelles consacrées aux licences ou aux abonnements Microsoft. Sur la base de ces données, l'État fédéral et les Länder pourraient prévoir beaucoup plus précisément les avantages tarifaires et les volumes dont ils ont besoin pour chaque exercice budgétaire. La collaboration entre les acheteurs informatiques de l'État fédéral, des Länder et des communes permettrait de réaliser des synergies et de réduire les asymétries d'information existantes vis-à-vis de Microsoft. Il est conforme au principe d'efficacité et d'économie de l'administration d'utiliser l'argent des contribuables de manière prudente et durable.

- **Adapter les modalités d'octroi des licences aux besoins de l'administration**

En vue des négociations sur un nouveau contrat-cadre avec Microsoft, l'État fédéral, les Länder et les

associations communales faîtières – par exemple dans le cadre du DMK ou du Conseil de planification informatique – devraient se préparer ensemble de manière très approfondie et, le cas échéant, faire appel à une aide extérieure. Cela implique au minimum de prévoir avec précision les besoins et les budgets respectifs, et de s'assurer du degré d'intérêt pour les solutions sur site, Microsoft365 ou le cloud public. En outre, l'État pourrait envisager de négocier des modifications du réseau de distribution existant par l'intermédiaire de Licensing Solution Partner et de jouer un rôle plus important dans l'octroi des licences.

- **Audits obligatoires et analyse transparente en temps réel des flux de données**

Le gouvernement fédéral devrait obliger Microsoft à permettre des audits approfondis donnant accès au code source avant que de nouvelles applications logicielles ou des mises à jour importantes ne soient utilisées dans l'administration publique. Seul un accès réel permet de vérifier si la protection des données sur papier correspond effectivement aux processus techniques dans la salle des machines. L'État peut garantir la confidentialité à l'entreprise. En outre, le gouvernement fédéral devrait s'engager à ce que tout accès à distance à l'infrastructure Microsoft fasse l'objet d'un enregistrement non modifiable. L'État devrait avoir une vue d'ensemble précise des accès au système, à savoir qui y a accédé, pour quelle raison et quelles données ont été transmises aux États-Unis.

- **Interopérabilité et interfaces ouvertes comme obligation contractuelle**

Sur la base d'études de faisabilité et des enquêtes menées par l'Office fédéral allemand des cartels, le gouvernement fédéral devrait déterminer dans quels domaines il peut obliger Microsoft, dans un contrat-cadre, à garantir l'interopérabilité avec d'autres produits et des interfaces ouvertes. Tant que l'écosystème Microsoft restera délibérément fermé et pourra jouer sur les effets de verrouillage, la dépendance se renforcera au lieu de diminuer.

Dans ce contexte, le gouvernement fédéral peut tout à fait menacer de se retirer des accords-cadres à une date butoir donnée si les négociateurs chevronnés du groupe Microsoft rejettent certaines exigences.

Mesures à long terme pour l'ère de la souveraineté numérique dans l'UE et en Allemagne :

Les années 1990, où il fallait choisir entre Apple et Microsoft, sont révolues depuis longtemps. Le marché informatique s'est fortement diversifié, même si cela ne se reflète pas dans les parts de marché de Microsoft dans le secteur public en raison de sa position dominante. À long terme, l'Allemagne a tout intérêt à mettre en place un système fonctionnel et interopérable avec différents fournisseurs et produits, une sorte de grand magasin informatique dans lequel les différentes administrations peuvent se servir et assembler la solution qui leur convient le mieux. Avec les initiatives « EuroStack » et « Deutschland Stack », dont le contenu n'est certes pas encore clairement défini, Bruxelles et Berlin se sont déjà engagées de manière programmatique sur la voie de la souveraineté numérique. Les paroles doivent bientôt être suivies d'actes. Il est important de tirer les leçons des échecs politiques tels que l'initiative « gaia x » et de ne pas répéter les mêmes erreurs.

À long terme, les gouvernements fédéral et régionaux devraient se poser la question suivante : les deniers publics qui sont dépensés chaque année en frais de licence pour les produits Microsoft ne seraient-ils pas mieux investis dans un réseau diversifié de fournisseurs informatiques, qui réduirait la dépendance excessive à l'égard d'un seul monopole et permettrait de mettre en place des solutions souveraines sur le plan numérique ?

À long terme, les gouvernements fédéral et régionaux devraient se poser la question suivante : les deniers publics qui sont dépensés chaque année en frais de licence pour les produits Microsoft ne seraient-ils pas mieux investis dans un réseau diversifié de fournisseurs informatiques, qui réduirait la dépendance excessive à l'égard d'un seul monopole et permettrait de mettre en place des solutions souveraines sur le plan numérique ? Il serait alors possible de créer un environnement logiciel et donc une base de travail numérique pour l'administration qui serait plus

facile à contrôler et à gérer pour l'État. Des autorités spécialisées telles que le BfDI, le Bundeskartellamt et le BSI pourraient définir les exigences en matière de protection des données, de sécurité informatique et de concurrence loyale, et accompagner leur mise en œuvre concrète. En conséquence, l'administration aurait la liberté de choix et pourrait planifier ses coûts à court, moyen et long terme. Pour garantir la cybersécurité, l'État ne serait plus tributaire de la confiance fragile accordée à Microsoft pour protéger ses systèmes contre les attaques.

Dans le meilleur des cas, cela créerait un environnement de travail numérique ouvert à la concurrence pour l'administration publique, auquel d'autres États voudraient également avoir recours : une pile allemande avec une communauté internationale, des services en constante évolution et les principes d'interopérabilité et de modularité comme essence de la marque. Sur la base de mesures à court et moyen terme, en particulier d'une base chiffrée valide sur les fonds publics utilisés et d'études de faisabilité, le gouvernement fédéral pourrait fixer une date à partir de laquelle la sortie de l'écosystème Microsoft vers un environnement de travail souverain pour l'administration devrait avoir lieu. Tous les acteurs pourraient alors aligner leurs plans stratégiques sur cette date de sortie. Mais ils ne le feront que s'il y a une « annonce claire venant d'en haut », dans le meilleur des cas de la part de la Chancellerie fédérale et des chancelleries d'État.

C'est un bon signe qu'un département entier consacré à la « pile allemande » soit prévu au sein du nouveau ministère fédéral allemand de la Numérisation et de la Modernisation de l'État (BMDS).

C'est un bon signe qu'un département entier consacré à la « pile allemande » soit prévu au sein du nouveau ministère fédéral allemand de la Numérisation et de la Modernisation de l'État (BMDS). Ce serait un succès international respectable pour le nouveau ministre fédéral, Dr Karsten Wildberger, s'il parvenait à faire passer l'Allemagne de la dépendance numérique à la souveraineté numérique. S'il parvient à mettre sur les rails, au cours de son premier mandat, le projet titanesque visant à sortir de la dépendance stratégique vis-à-vis des produits

Microsoft, et s'il est prêt à tenir tête au géant technologique Microsoft, jusqu'ici presque intouchable (), dans la mesure où cela sert les intérêts de l'État allemand, il aurait alors fait honneur à sa réputation de gestionnaire de crise pour les grands projets informatiques. Ce ne serait pas seulement un succès politique, mais aussi, dans le meilleur des cas, un programme de relance économique pour l'économie numérique nationale et un gain précieux en termes de liberté de choix et de décision numériques pour tous.



Mentions légales

L'auteur

Michael Kolain est juriste et expert en politique numérique. Il travaille à l'interface entre la législation, la science et le développement des technologies numériques.

cyberintelligence.institute (éditrice)

MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

T +69 5050 34-602

www.cyberintelligence.institute
info@cyberintelligence.institute

Le texte de cet ouvrage est sous licence selon les conditions de „Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 4.0 international“, CC BY-SA 4.0 (disponible à l'adresse : <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>)