Dépendances technologiques : un risque de gouvernance à maîtriser

Alors que la question de la souveraineté technologique relève d'abord de l'État, les entreprises doivent aujourd'hui se concentrer sur la notion de dépendances stratégiques pour en appréhender les risques et assurer la résilience et l'autonomie stratégique de leur système IT.

Un travail d'autant plus nécessaire pour les entreprises européennes particulièrement vulnérables du fait de la dépendance systémique de l'Europe aux technologies numériques et digitales venues des États-Unis.

David KRIEFF

Directeur du digital et de la transformation GROUPE ADP

À vrai dire, pourquoi une entreprise s'intéresserait-elle au sujet de la souveraineté technologique qui relève plutôt des attributions de l'État ? Et alors même que cette notion de souveraineté ne s'écrit pas au singulier pour les entreprises qui opèrent à l'international et qui doivent en conséquence se conformer aux cadres normatifs des différents pays.

Pour autant, toutes les entreprises devraient aujourd'hui se soucier de leur résilience numérique, sachant que le coût de cette dépendance technologique pour les entreprises européennes se chiffre en centaines de milliards d'euros par an. Certaines directives européennes comme le DORA (Digital Operational Resilience Act) dans le secteur financier vont jusqu'à pointer la responsabilité personnelle des dirigeants et des administrateurs en la matière. Mais pour que les instances de gouvernance de l'entreprise (conseil d'administration, Comex, etc.) puissent correctement en apprécier les risques, encore faut-il que les DSI puissent aider et éclairer sur les impacts potentiels de telle ou telle dépendance technologique et sur les options disponibles pour y faire face.

Cartographier les dépendances technologiques : un enjeu majeur pour l'entreprise

Le concept le plus opérant à l'échelle de l'entreprise est celui de l'autonomie stratégique, qui suppose d'effectuer en amont une cartographie des dépendances technologiques. Un travail indispensable pour qu'ensuite, l'entreprise puisse s'appuyer sur un socle IT solide sans fragilité structurelle ou craintes d'être remis en cause par des facteurs exogènes : politique commerciale des éditeurs de logiciels (ce n'est faire injure à ces deux sociétés que de rappeler que parfois les négociations avec SAP ou Microsoft peuvent

parfois être difficiles), disruption sur la chaîne d'approvisionnement, tensions géopolitiques, etc. Sur ce dernier point, l'utilisation des outils de souveraineté par les États à des fins géopolitiques peut constituer un risque pour les entreprises.

La cartographie des dépendances numériques et technologiques apparait donc comme la pierre angulaire sur laquelle repose la résilience des systèmes IT. Pour mesurer cette dépendance, certaines entreprises utilisent ce qu'on appelle l'indice de résilience numérique : une initiative de place sous le patronage de l'ancienne ministre du numérique, Clara Chappaz. Ainsi, plusieurs risques sont passés au crible : la dépendance à tel ou tel fournisseur, à une technologie en particulier, à un flux d'approvisionnement, etc.

Des obligations pouvant conduire à des conflits de souveraineté

La souveraineté et la dépendance technologique peuvent influencer directement la bonne marche et les activités de l'entreprise, en particulier dans deux cas de figures.

Le premier cas relève d'une entreprise qui opère sur un marché par nature souverain, comme le secteur de la défense et de l'armement, pour lequel le portefeuille européen d'identité numérique s'applique en vertu du règlement eIDAS 2 (Electronic Identification And Trust Services). Dans ce cadre, l'État exerce sa souveraineté sur les technologies que l'entreprise utilise. En France, la loi de programmation militaire (LPM) identifie les opérateurs d'importance vitale (OIV), qui doivent recenser en leur sein les systèmes d'information d'importance vitale (SIIV) auxquels s'appliquent alors des obligations spécifiques. L'article 22 de la LPM impose par exemple de garantir l'autonomie stratégique des SIIV, notamment en évitant l'intégration de composants ou de services soumis à des législations extra-européennes.

Le second cas est celui d'une entreprise qui doit faire face à deux logiques de souveraineté contradictoires. Par exemple, le cas d'une institution financière européenne qui opère en Europe et recours aux services d'un *hyperscaler*[1] américain. Si celui-ci est victime d'un événement cyber paralysant les opérations financières et que cet événement est classé comme sensible par les autorités américaines, l'*hyperscaler* a l'interdiction

de communiquer la moindre information à ce sujet. De fait, la banque européenne est dans l'impossibilité de satisfaire à son obligation d'information (directive DORA) et de transparence auprès de l'autorité de supervision (ACPR ou BCE) et elle s'expose, ainsi que ses administrateurs, à d'éventuelles sanctions.

Ces deux cas de figures démontrent que la cartographie des dépendances technologiques est un préalable nécessaire, pour pouvoir gérer les risques en matière de souveraineté.

Des outils de souveraineté à des fins d'intelligence économique

La souveraineté peut aussi impacter les entreprises par le biais du Cloud Act et du FISA (Foreign Intelligence Surveillance Act) américains. Cette dernière loi américaine stipule que la communauté du renseignement des États-Unis peut collecter des communications électroniques d'entités non-américaines, même situées à l'étranger et sans mandat individuel (dans le cadre par exemple de la lutte anti-terrorisme ou d'autres atteintes à la sécurité nationale). Même en étant localisées sur des serveurs européens, les données collectés se retrouvent alors stockées dans les *clouds* d'hyperscalers américains (Microsoft Azure, Google GCP, Amazon AWS), faisant peser le risque d'être utilisés à des fins d'intelligence économique. Certaines entreprises non américaines craignant pour leurs datas privilégient des *clouds* qui ne sont pas exposés à ces dispositions extraterritoriales du droit américain. En France, l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Informations)

1. Les *hyperscalers* sont les géants du cloud : Amazon avec AWS, Microsoft avec Azure et Google avec GCP.

recommande d'ailleurs aux OIV, d'avoir recours à des *clouds* qui disposent d'une protection contre les législations extraterritoriales.

La Chine dispose d'un arsenal législatif au moins équivalent à celui des États-Unis. La loi sur le renseignement national prévoit une obligation de coopération qui oblige toutes les organisations et citoyens chinois à soutenir, assister et à coopérer avec les services de renseignement chinois, ce qui inclut la fourniture de données.

La dépendance systématique de l'Europe aux États-Unis coûte cher

Face à une rivalité technologique mondiale qui tend à s'exacerber, l'Europe pêche aujourd'hui par une insuffisance de souveraineté et de moyens. Publiée en 2025, une étude[2] du cabinet Astérès, conduite pour le Cigref, met évidence que 83 % des dépenses des entreprises européennes liées aux logiciels et services-cloud à usage professionnel sont investies outre-Atlantique. L'étude chiffre, pour la première fois, le montant de cette dépendance à 264 milliards d'euros, soit 1,2 % du PIB européen. En outre, elle estime que si l'Union européenne parvenait, en 2035, à produire 15 % des services de cloud-logiciel qu'elle achète actuellement aux États-Unis, cela entraînerait la création d'environ 463 000 emplois en Europe, et aurait un effet positif de 0,2 point (37 Md€) sur le PIB de la zone.

La technologie ayant pris une place prépondérante, nos sociétés fonctionneraient très difficilement sans logiciels de bureautique, messageries et mails, annuaires de sécurité, *clouds*… Or quasiment tous ces outils émanent d'entreprises américaines. Prenons l'exemple des systèmes de paiement électronique. Rares sont les pays qui disposent d'une infrastructure de paiement électronique en propre, comme la France avec le groupement carte bleue. La plupart des pays ont recours à Visa, Mastercard ou American Express pour les paiements par carte bancaire. D'ailleurs, les paiements transfrontaliers au sein du marché unique européen se font via ses services sous souveraineté extra-européenne, dont l'accès - s'il venait à être interrompu – poserait de sérieux problèmes. Un scénario qui n'est pas irréaliste car, dans la pratique, le pouvoir exécutif américain peut exclure n'importe quel citoyen européen du système bancaire et de l'espace numérique de son propre pays. C'est le cas depuis août 2025, du juge français de la Cour Pénale Internationale (CPI), Nicolas Guillou et d'autres magistrats de la CPI, qui sont visés par un décret présidentiel de Donald Trump, interdisant à toute personne physique ou morale américaine, y compris leurs filiales à l'étranger, de leur fournir des services à titre onéreux ou gratuit. Par conséquent, ces magistrats ne peuvent plus utiliser les services de Visa, Mastercard, Airbnb, Amazon, Paypal, etc.

Des leviers pour une tech européenne plus performante

Alors comment se prémunir face à de tels risques de dépendance ? Une fois les dépendances technologiques cartographiées, la solution serait pour l'entreprise de diversifier autant que possible ses fournisseurs et achats de prestations intellectuelles. Mais à la part d'achats massifs réalisés outre-Atlantique répond actuellement la faiblesse de l'offre européenne en matière numérique et digital. Abandonner les outils et technologies américaines auxquels nous sommes habitués et dont maîtrisons les usages n'est pas facile et pourrait nuire à la performance, du moins à court termes en l'absence de technologies européennes aussi efficientes. Dit autrement, la souveraineté européenne sur les technologies du numérique doit aller de pair avec la construction d'un écosystème industriel robuste et compétitif.

Les leviers existent pour que l'Europe se dote enfin d'une politique industrielle numérique commune qui soit davantage au service de ses

2. https://www.cigref.fr/wp/wp-content/uploads/2025/04/Etude-Asteres-La-dependance-technologique-aux-services-de-cloud-et-logiciels-americains-avril-2025.pdf

propres intérêts. Citons par exemple, l'adoption d'une règlementation européenne intégrant les nouveaux enjeux (IA et autres), des dispositifs de financement de l'innovation plus conséquents pour faire émerger des champions technologiques européens. Le rôle accru de la commande publique dont l'effet serait double : d'une part, des marchés publics substantiels stabiliseraient les ressources et la stratégie d'acteurs émergents et d'autre part, cela enverrait un signal fort aux commanditaires privés qui pourraient avoir confiance dans la pérennité et la robustesse des acteurs de la tech européenne. Autre levier, l'ajout de briques technologiques (digital commons) au travers d'instruments de coopérations que sont les EDIC (European digital infrastructure consortium). Les grandes entreprises, par la taille importante de leur DSI, pourraient y contribuer.

Le dernier levier reste trop souvent ignoré : changer de regard et avoir une communication plus positive sur les technologies européennes. Dans les années 2000, les entreprises françaises de la tech étaient jugées trop grosses pour rivaliser avec l'agilité des startups alors qu'aujourd'hui elles sont trop petites face aux GAFAM et autres géants américains de la tech. Le point commun entre ces deux périodes est que nous avons laissé s'installer une perception défavorable, en partie auto-réalisatrice.

Enfin, il existe de bonnes raisons pour appeler de ses vœux la constitution d'un écosystème technologique européen mieux organisé et aligné avec ses intérêts. Le développement des compétences numériques qui en résulterait rejaillirait sur les entreprises qui ont besoin de disposer d'un vivier de talents. Les entreprises de la tech européenne pourraient aussi apporter de l'eau au moulin des travaux législatifs pour bâtir un cadre réglementaire et institutionnel européen qui, plus que la production de normes parfois contraignantes, encourage réellement l'innovation et la prise de risques.

Disposer d'un écosystème technologique vigoureux en Europe serait un réel atout, et les entreprises européennes peuvent contribuer à son émergence. Mais la responsabilité première des entreprises s'incarne d'abord et avant tout dans la gestion lucide de leurs dépendances technologiques, condition sine qua none pour tendre vers une autonomie stratégie en matière d'IT. ■