Maîtriser la donnée sensible pour répondre aux exigences du *contrôle des exportations*

Capgemini invent

Introduction

La recrudescence des conflits armés (Ukraine, Moyen-Orient), ainsi que la guerre économique latente entre les grandes puissances (US, Chine, Europe) confirment aujourd'hui l'importance, vitale pour les gouvernements, de maîtriser et de contrôler les exportations.

Le contrôle des exportations recouvre un ensemble de règles qui, d'un côté, concourent à la sécurité des nations dans le contrôle des armes; de l'autre côté, qui protègent les intérêts économiques et stratégiques des pays (technologies d'Intelligence Artificielle, quantiques, les biotechnologies, les semi-conducteurs, etc.) pour les biens et technologies dits à « double usage » (civil et militaire).
Le non-respect de ces règles peut donner lieu à un ensemble de sanctions de différentes natures :

- **Financières** : amendes et pénalités monétaires (jusqu'à 10% du chiffre d'affaires de l'entreprise)
- **Commerciales** : exclusion d'accès à des ressources, exclusion de participation à certains marchés, interdiction de commercer en dollars, pénalités contractuelles
- **Réputationnelles** : perte de crédibilité face aux clients et aux autorités, dommages réputationnels vis-à-vis des actionnaires, des régulateurs et de l'opinion publique.
- **Pénales** : emprisonnement de dirigeants

Les autorités sont de plus en plus vigilantes à la conformité des entreprises et ont renforcé leurs sanctions ces dernières années.

En effet, des sociétés de premier plan (Airbus, Alstom, Boeing, Honeywell, BAE Systems, …) ont payé des pénalités d'un montant significatif, pouvant atteindre plusieurs centaines de millions de dollars, aux autorités américaines, françaises et britanniques, pour solder leurs contentieux. C'est pourquoi le sujet se retrouve sur la table des CxO dans le secteur de la défense, mais également dans d'autres industries (aéronautique, nucléaire, chimie, électronique, naval, ferroviaire, énergie, services, etc).

Pour ces raisons le contrôle à l'exportation est un sujet d'actualité dont la complexité (prise en compte de multiples juridictions) et l'évolutivité demandent une capacité d'adaptation continue des entreprises. Il est crucial d'apporter une réflexion méthodologique structurée pour accompagner ces acteurs économiques dans leur engagement de conformité. Le présent document n'évoque pas le cadre légal et juridique de la mise en conformité, mais il donne les clés de compréhension aux responsables de programme de conformité sur la gestion de la donnée contrôlée et quelles sont les étapes pour en assurer sa conformité aux régulations.

La maitrise de la donnée contrôlée s'étend sur une longue période, autour de trois piliers :

- L'**urgence** : identifier, classer et isoler les données contrôlées pour palier le risque d'envoi non autorisé de données.
- L'**impératif** : à moyen terme, restreindre l'accès à la donnée contrôlée aux seuls individus autorisés pour empêcher tout risque de brèches de conformité.
- La **finalité** : à long terme, mettre en œuvre la continuité digitale entre les différents systèmes pour répondre de manière plus systématique aux exigences réglementaires.

Quelques éléments de rappel sur le contrôle des exportations

Le contrôle des exportations est un ensemble de lois et de réglementations qui régissent les transferts de biens et technologies à travers le monde. Tout employé y étant exposé est soumis à des droits et des devoirs relatifs à l'utilisation qui est faite de cette technologie, pour des raisons relatives à la sécurité nationale, à la politique étrangère, ou à tout autre objectif national.

Différents cadres réglementaires existent en fonction du pays exportateur et de la typologie du bien contrôlé (militaire, à double usage).

Qu'est-ce qu'un export ?

On entend par export tout envoi physique, transmission digitale, publication, mise à disposition physique ou utilisation effective d'un bien contrôlé, au titre ou pour le bénéfice d'une entité ou d'une personne étrangère.
Par exemple, un fournisseur dans un pays A envoie un matériel con-trôlé à un client dans un pays B.

Dans le cadre de la règlementation américaine, d'autres formes d'export sont définies à travers des mesures extraterritoriales :

- Le re-export : export d'un bien contrôlé, dont l'origine première est américaine, vers un pays tiers.
- Le re-transfert : correspond au mouvement à l'intérieur d'un pays d'un bien contrôlé, dont l'origine première est américaine, vers une nouvelle entité juridique.
- Le re-export présumé : correspond au partage d'un bien contrôlé d'origine américaine avec un collègue d'une même entité juridique mais dont la nationalité diffère de celle de l'entité juridique, à l'exception de la nationalité américaine.

Qu'est-ce qu'un bien contrôlé ?

Par bien contrôlé, on entend équipement matériel, donnée technique, logiciel, service, transfert de responsabilité à des tierces parties, opération de courtage. Sont ainsi exportés des biens physiques (tangibles) et de l'information technique (intangible). Dans ce point de vue, nous focalisons notre attention sur la partie intangible (information technique).

Qu'entend-on par information technique ?

Une information technique est une donnée ou un ensemble de données qui fournissent des détails spécifiques sur le fonctionnement, la conception, l'utilisation ou la maintenance d'un produit, d'un système ou d'un processus.
Il s'agit par exemple de dessins 3D, un croquis, manuel d'utilisation, rapports de test, demandes de modification d'un produit, cahiers des charges, instructions de production, instructions de maintenance.

Par opposition, voici quelques exemples d'information non technique : contrat et avenant au contrat de travail, états financiers, documents de gestion de projet (budget, planning, risques, plan de communication, identification des parties prenantes, etc.), certificats de conformité.

La France comme origine de l'Export Control (?)

Il est généralement admis que les États-Unis tiennent le rôle précurseur de cette réglementation depuis la guerre froide. Cependant, depuis la naissance des États, des formes basiques de contrôle des exportations ont toujours existé. Dès le VIIIe siècle, Charlemagne a interdit l'exportation en dehors de l'empire Carolingien des épées franques, dont l'alliage spécifique d'acier apportaient une véritable suprématie aux armées. Il a même interdit aux forgerons qui maîtrisaient cette technique de voyager en dehors de l'Empire. C'est la première occurrence documentée d'une décision étatique visant à contrôler l'exportation de produits militaires (édit de Pistres en 864) !

L'*urgence* : identifier, classer et isoler les données contrôlées pour palier le risque d'envoi non autorisé de données.

Il s'agit de répondre à trois questions essentielles :

- Quelles sont les données qui sont contrôlées et celles qui ne le sont pas ?
- Où se situent ces données contrôlées dans mon système d'information ?
- Quel est le plan tactique de conformité à mettre en place pour assurer la bonne cascade des exigences légales vers des solutions opérationnelles ?

Une **approche structurée** est nécessaire avec pour prérequis l'établissement d'une **carte applicative et fonctionnelle**, avec l'appui des différents métiers de l'entreprise. Cela permet une vue claire du portefeuille applicatif et des flux de données entre applications. Puis :

- **Identifier** dans une vision macroscopique les applications et les objets métiers qui font l'objet d'Export Control. Il faut donc analyser finement les applications et les objets métier, afin de qualifier et valider ceux qui sont réellement porteurs de données contrôlées.
- **Classer** la donnée à sa création, sa modification dans les outils, ou lors de sa réception venant de systèmes extérieurs (si elle n'est pas déjà classée). Le classement repose sur une ontologie pour pouvoir classer de manière précise et rigoureuse la donnée selon les exigences des réglementations de contrôle d'exportation. Dans le choix de l'architecture de la solution apparaît la contrainte de la propagation d'un classement d'un système applicatif à un autre. Il faut également s'assurer que le dernier classement de la donnée peut être remonté à tout moment. Bien souvent il s'agit d'un dilemme à résoudre au cas par cas entre une gestion locale de la propagation (moins coûteuse mais moins robuste à l'échelle) et une solution globale. La complexité de cette étape réside dans la diversité des technologies qui peuvent exister au sein d'un système d'information chez un industriel, entre des solutions de PLM, ERP, CRM, pour ne citer que ces composants majeurs.
  Puis, annoter visuellement les documents sensibles via des logiciels dédiés (existants sur le marché, ou développés spécifiquement), pour faire en sorte que la régulation applicable au document soit visible et explicite pour toute personne ouvrant le document.
- **Isoler** la donnée contrôlée, en la ségrégant dans des volumes de stockage spécifiques qualifiés à cet effet, ce qui peut être fait par le responsable informatique de l'application.

Dans certaines industries où le nombre de données est volumineux, le défi est également de trouver une solution pour classer les données déjà existantes. Il peut s'avérer onéreux de se lancer dans une activité de classement de toutes les données, de ce fait une stratégie de classement lors de la modification de la donnée (lorsque qu'elle se produit) peut être le meilleur compromis.

Lorsque des volumes importants de données sont à traiter, des solutions de science de la donnée peuvent aider à la décision. Des mécanismes de GenAI peuvent compléter le dispositif en apportant une aide dans la proposition de classement (par exemple au travers d'un Chatbot connecté à un modèle de langage contextualisé).

Il nous semble important de souligner dans cette phase le rôle clé porté par l'**architecture d'entreprise**. La mise en conformité au contrôle des exportations suppose une lecture et une analyse détaillées de l'architecture d'entreprise, pour comprendre les attendus en matière d'adaptabilité du système d'information, et ainsi décliner une vision propre de la conformité au sein du projet d'entreprise. L'inscription de la mise en conformité dans la vision d'architecture d'entreprise permet de confronter les exigences de contrôle des exportations avec la réalité des enjeux opérationnels et commerciaux.

L'*impératif* : à moyen terme, restreindre l'accès à la donnée contrôlée aux seuls individus autorisés pour empêcher tout risque de brèches de conformité

Dès que nous savons où se trouve la donnée contrôlée et quel est son classement, l'impératif est de restreindre son accès aux seuls individus qui en ont « le besoin » et le « droit d'en connaître ». Pour ce faire il faut pouvoir se doter de mécanismes autorisant les individus à accéder à la donnée.

Comment gérer les droits d'accès individuels à la donnée contrôlée ?

Il faut tout d'abord **identifier** les personnes qui veulent accéder ou qui ont déjà accès à l'application contenant la donnée contrôlée visée. Cette étape peut être plus ou moins complexe, en fonction du mode de gestion des identités des utilisateurs (gestion dans un annuaire centralisée, ou gestion décentralisée).

Ensuite il faut mettre en œuvre un procédé d'autorisation au niveau utilisateur, sous la forme d'**accréditation** personnelle. Cette autorisation se fait à deux niveaux :

- Elle valide le « besoin d'en connaître » de l'individu à travers des vérifications au niveau des contrats de collaboration, sous-traitance et co-traitance ;
- Elle valide le « droit d'en connaître » de l'individu (nationalité, société de rattachement par rapport à une ou des listes d'autorisations accessibles sur les licences accordées par les autorités étatiques).

Ce mécanisme doit être automatisé afin de limiter les actions manuelles, souvent sources d'erreurs. Cela impose à l'entreprise d'avoir des référentiels d'identité et de licences exhaustifs et régulièrement entretenus.

Comment autoriser les accès aux seules personnes autorisées ?

La sécurisation via des moyens technologiques peut se faire à différents niveaux :

- Au niveau de l'application dans le cas où il n'y a pas de ségrégation dans l'application. Il faut mettre en place des briques logicielles qui permettent de vérifier les droits d'un utilisateur lors de sa connexion à l'application.
- Au niveau du conteneur de données, dans le cas d'une ségrégation à niveau moyen. C'est par exemple le cas des répertoires de stockage. Limiter leurs conditions d'accès aux personnes qui ont le « droit d'en connaître », c'est le rôle du responsable métier de l'application, en lien avec le département juridique, qui aidera à poser les bases légales des autorisations (à travers des licences).
- Au niveau de la donnée, dans le cas d'une ségrégation à **niveau fin**. Dans ce cas, il est souvent nécessaire d'intégrer des solutions de marché, qui permettent d'opérer ces mécanismes de contrôle d'accès à la donnée unitaire. C'est un investissement consé-quent pour l'entreprise, mais c'est la solution la plus précise et pérenne, tout en limi-tant les contraintes opérationnelles.

Lorsque des moyens technologiques ne peuvent être mis en œuvre, il faut contrôler de manière régulière (hebdomadaire ou mensuelle suivant le volume d'utilisateurs, et le risque d'exposition des données contrôlées) les accès des personnes à ces applications, ce qui relève également du responsable métier de l'application.

Certaines règlementations imposent de contrôler le lieu d'accès à la donnée grâce à la géolocalisation de l'utilisateur et d'en restreindre son accès en fonction du pays. Avec la complexité croissante des infrastructures informatiques, notamment dans le cas où l'entreprise travaille en entreprise étendue avec des fournisseurs installés à plusieurs endroits du globe, cette tâche peut se révéler ardue.

La *finalité* : à long terme, mettre en œuvre la continuité digitale entre les différents systèmes pour répondre de manière plus systématique aux exigences réglementaires

Un programme de conformité doit viser l'effectivité, l'efficacité et la preuve du contrôle, la prédictibilité des potentielles failles de conformité, et la livraison de rapports précis et fiables pour les autorités. De ce fait tout responsable de programme de conformité dans l'entreprise doit tirer parti de la **continuité digitale** pour bénéficier de 3 leviers majeurs :

- La **résilience** : les données étant généralement traitées, copiées, propagées manuellement, une source importante de brèche de conformité repose sur les erreurs humaines. La continuité digitale conditionne une gouvernance stricte de la donnée qui assure sa fiabilité en toute occasion.
- La **traçabilité** : disposer de moyens digitaux liant une donnée à sa juridiction, aux utilisateurs et sociétés (incluant leurs autorisations d'accès), aux licences sous-jacentes, permet un meilleur contrôle du système global.
- L'**adaptabilité** : l'évolution rapide des règlementations impose une adaptation fluide et agile de l'entreprise. La continuité digitale permet d'organiser la cascade des changements de directives dans l'ensemble du système de gestion de l'entreprise.

Actuellement et encore plus dans un futur proche, les dernières avancées technologiques, comme **l'intelligence artificielle (IA)** – générative ou non – sont des aides majeures pour la conformité à l'Export Control. Elles vont permettre d'accélérer les opérations de conformité, par exemple via l'utilisation de GenAI pour aider à une proposition de classement de la donnée, ou aider à la compréhension de changement de régulations. Notons toutefois que l'IA est en elle-même un enjeu de conformité, dans un optique de double usage.

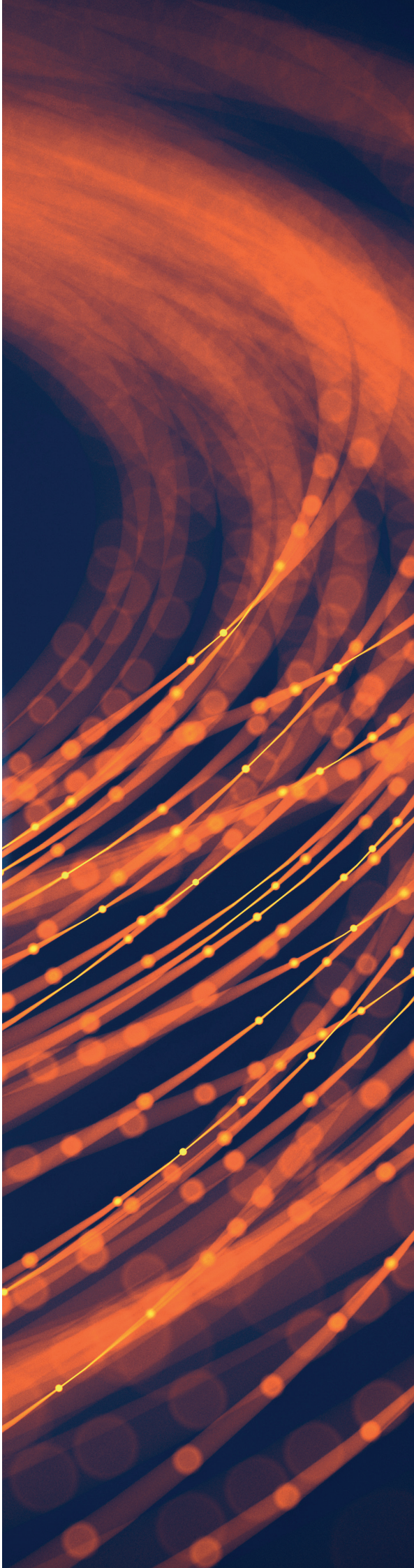
Conclusion

La situation géopolitique actuelle incite les Etats à davantage réguler et contrôler les biens et technologies qu'ils exportent, qu'il s'agisse de matériels militaires ou de technologies sensibles à double usage dans un but de souveraineté économique. Cela affecte la macro-économie mondiale, comme les difficultés rencontrées par le modèle d'exportation allemand et cela explique la montée en puissance de pays d'Asie du Sud-Est comme alternative à la Chine.

La conformité au contrôle des exportations est de premier plan et se révèle être perpétuelle pour les entreprises, avec de multiples règlementations évoluant rapidement. Conserver une autonomie et une sécurité de développement à l'international requiert d'agir avec vigilance dans le choix des clients, partenaires ou fournisseurs, voire des collaborateurs.

Répondre à l'urgence d'identifier la donnée, s'engager sur l'impératif d'y restreindre son accès aux seules personnes autorisées, tout en visant la finalité d'une continuité digitale qui limitera grandement les brèches de non-conformité, voilà la feuille de route à laquelle tout responsable de mise en conformité de l'entreprise peut souscrire.

Dès lors le / la responsable d'un programme de conformité devra s'assurer d'une parfaite orchestration entre les acteurs du Légal, les acteurs du Digital et les métiers de l'entreprise, pour réussir à bâtir et engager largement sur ce chemin de conformité. C'est aussi une opportunité inédite pour l'entreprise de redécouvrir et maitriser en profondeur l'architecture de son système d'information.
Nos recommandations rentrent par ailleurs dans une démarche systémique qui peut être communalisée avec d'autres besoins de conformité (CSRD, AI Act, etc).



Auteurs

Mikael CARASSOU-MAILLAN
VP Aerospace & Defense
mikael.carassou-maillan@capgemini.com

Mikel BADIOLA
Principal Aerospace & Defense
mikel.badiola@capgemini.com

Sebastien HULLAERT
Principal Aerospace & Defense
sebastien.hullaert@capgemini.com

Nicolas PIVETEAU
Managing Consultant Aerospace & Defense
nicolas.piveteau@capgemini.com

A propos de Capgemini Invent

Capgemini Invent est la marque d'innovation digitale, de design et de transformation du groupe Capgemini, qui permet aux dirigeants de façonner l'avenir de leurs entreprises. Etablie dans plus de 30 studios et plus de 60 bureaux dans le monde, elle comprend une équipe de plus de 12 500 collaborateurs, composée d'experts en stratégie, de data scientists, de concepteurs de produits et d'expériences, d'experts en marques et en technologie qui développent de nouveaux services digitaux, produits, expériences et modèles d'affaire pour une croissance durable.

Capgemini Invent fait partie du groupe Capgemini, partenaire de la transformation business et technologique de ses clients, les accompagne dans leur transition vers un monde plus digital et durable, tout en créant un impact positif pour la société. Le Groupe, responsable et multiculturel, rassemble 340 000 collaborateurs dans plus de 50 pays. Depuis plus de 55 ans, ses clients lui font confiance pour répondre à l'ensemble de leurs besoins grâce à la technologie. Capgemini propose des services et solutions de bout en bout, allant de la stratégie et du design jusqu'à l'ingénierie, en tirant parti de ses compétences de pointe en intelligence artificielle, en cloud, et en data, ainsi que de son expertise sectorielle et de son écosystème de partenaires. Le Groupe a réalisé un chiffre d'affaires de 22,5 milliards d'euros en 2023.

Get the future you want*

Plus d'informations sur www.capgemini.com/invent

* *Réalisez le futur que vous voulez*

Capgemini invent