# L'ENCADREMENT JURIDIQUE DU PARTAGE DE LA DONNEE RH À LA DIRECTION DES RESSOURCES HUMAINES DU MINISTERE DES ARMEES : L'EXEMPLE DE SOURCEWEB

*Par le Lieutenant-colonel Bertrand PROUT,*
*en master 2 « Gestion RH et management public »*
*à l'université Panthéon-Assas au titre du Brevet Technique*

Le partage de la donnée est un enjeu majeur pour le ministère des Armées et l'API[1] en est l'outil principal.
Toutefois, en matière de ressources humaines spécifiquement, si le droit a bien envisagé et encadré la protection des données personnelles exploitées dans le cadre d'un traitement papier ou informatique, le **partage de la donnée par API** rebat les cartes des rôles, obligations et responsabilités de chacun des acteurs.

Comme les chefs de projets, les juristes doivent faire preuve d'agilité pour répondre aux avancées technologiques et numériques tout en respectant la règlementation dans l'intérêt bien compris de l'agent, sujet du traitement et des impératifs d'une gestion performante donc digitalisée.

Ainsi, nous expliquerons tout d'abord succinctement en quoi le partage de la donnée est un impératif pour l'État et particulièrement pour le ministère des Armées (**A**). Puis, nous recentrant sur la donnée Ressources Humaines, nous poserons le cadre juridique du traitement des données personnelles (**B**) pour enfin nous intéresser, en nous appuyant sur l'exemple de l'interface SourceWeb, sur la réponse apportée par le ministère des Armées à la question du partage de la donnée RH et l'agile élaboration de son cadre juridique et réglementaire qui l'a accompagnée (**C**).

*
* *

## A. Le partage de la donnée : un impératif stratégique dans le cadre de la transformation numérique de l'État.

Les données sont la richesse du XXI[ème] siècle, un « *actif stratégique* » de toute organisation. Couplées aux algorithmes, elles constituent « *les carburants de l'intelligence artificielle* » (IA)[2]. Les premières applications de cette IA dans le domaine civil contribuent déjà considérablement à l'amélioration des services publics[3].

---

[1] *Application Programming Interface,* interface informatique
[2] Discours « Intelligence artificielle et défense », Florence Parly, ministre des Armées, 5 avril 2019, Saclay. « *Nous investirons d'abord dans les carburants de l'IA : c'est-à-dire les données et les capacités de calcul… Ces données ne seront plus perdues ou gaspillées faute d'outils pour les recueillir, les stocker ou les traiter… Nous prendrons le virage du* cloud *pour disposer des capacités de calcul et de stockage indispensables au développement de l'IA, sans compromettre la sécurité et la souveraineté de nos données. Il nous faudra décloisonner les données, les partager, en faire un actif stratégique de notre ministère* »
[3] Citons par exemple, le **filtrage des appels d'urgence** arrivant aux 17-18-112 pour désaturer, mieux prioriser et cibler les interventions ou bien la **gestion de crise** par la gestion des interventions et de l'information ou encore la **réduction de l'accidentologie** et du nombre de morts sur les routes

En conséquence, promouvoir la culture de valorisation des données, accroître la « *datalphabétisation* »[4] des agents, faire du Ministère des Armées un ministère piloté par les données (« *data-driven »)*, utiliser les nouvelles technologies et les innovations numériques comme levier de performance, explorer toutes les applications opérationnelles et concrètes du traitement massif de données (« *Big Data* ») et de l'intelligence artificielle, figurent parmi les nombreux défis à relever[5].

Parmi ces missions, la culture de valorisation des données se concrétise dans le quotidien de nos concitoyens dans le principe du « *Dites-le-nous une fois* » - DLNUF – qui consiste à leur éviter, lors de leurs démarches en ligne avec une administration française, de fournir des informations ou pièces justificatives déjà détenues par d'autres administrations. Et cela, grâce au partage automatique de données via des API. À titre d'illustration de ce principe, le service d'authentification FranceConnect permet à nos concitoyens, grâce à un identifiant unique, d'accéder à plus de 900 formulaires préremplis des informations déjà communiquées sur l'un des services (impôts, retraites, famille, titres, santé, énergie) ; ils peuvent également choisir de se constituer un coffre-fort de documents qui pourront être utilisés dans différentes démarches.

Le succès de ces missions de fond sous-tend la réussite complète de la transformation numérique du ministère des Armées, notamment en matière de ressources humaines avec le futur SIRH ministériel, et plus largement de l'État. Néanmoins ce succès ne peut être remporté à n'importe quel prix, particulièrement s'agissant des données personnelles des individus sujets des traitements.

## B. L'indispensable protection des données personnelles

Avant de décrire les mécanismes de protection juridique des données personnelles, il est indispensable de poser quelques définitions :

- Au regard du droit en vigueur[6], est considérée comme une donnée personnelle toute information se rapportant à une personne physique identifiée ou qui peut être identifiée directement ou indirectement par référence à un identifiant[7].
- Un traitement de données quant à lui, est une opération ou un ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé (automatisé ou non), dans les sphères professionnelle et sociale[8].

Pour pouvoir se servir de données personnelles, le traitement doit respecter les 6 principes fondamentaux du traitement des données :

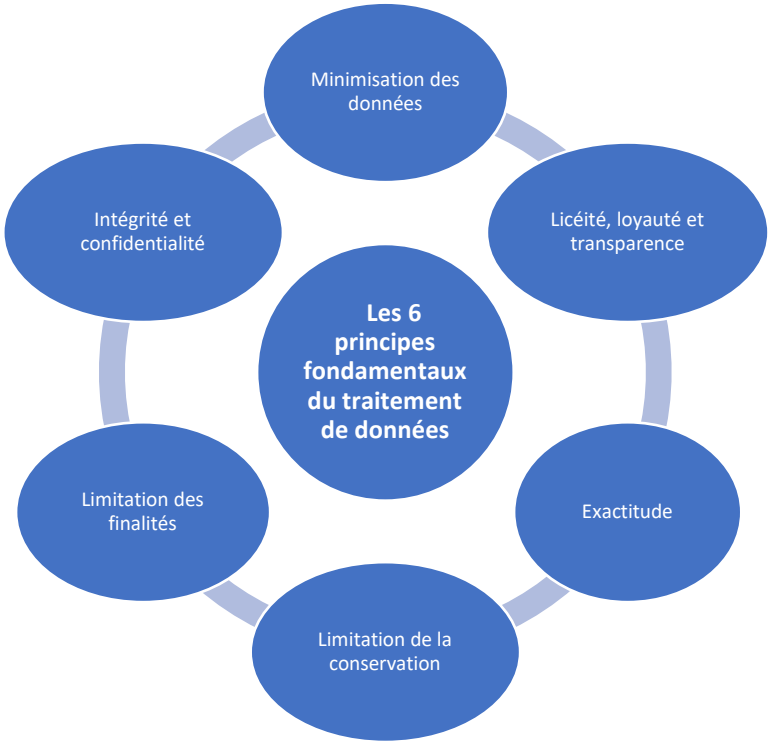
[4] Capacité des agents à utiliser les données dans leur quotidien

[5] Cf. *La donnée, prérequis au Big Data et à l'intelligence artificielle*, VA Arnaud Coustillère *in* Revue Défense Nationale 2019/5 (N°820), pages 43 à 48

[6] En l'occurrence le Règlement Général sur la Protection des Données – RGPD- du 27 avril 2016 et la Loi relative à la protection des données personnelles du 14 mai 2018

[7] Exemples de données personnelles : CV, coordonnées privées, numéro RIB, numéro de sécurité sociale, photo d'identité, justificatifs médicaux, adresse courriel, situation de famille, bulletins de paie, suivi médical…

[8] Exemples de traitement : collecte, consultation, adaptation/modification, transfert, effacement. En sont exclus les traitements pour des motifs personnels ou privés




Enfin, les protagonistes clés, interlocuteurs de la Commission Nationale Informatique et Libertés (CNIL) sont le responsable de traitement (RT) et le délégué à la protection des données (DPD). Le RT détermine les finalités et les moyens du traitement tandis que le DPD informe et conseille sur les obligations légales, contrôle la conformité du traitement à la règlementation, assiste pour les études d'impact et vérifie qu'elles sont réalisées tout en étant le point de contact privilégié de la CNIL[9].
Ils doivent tenir à jour un registre des activités de traitement de leur organisme[10] ainsi que, pour chacun des traitements, une analyse d'impact protection des données (AIPD)[11].

La mise en œuvre de cette règlementation est contraignante mais raisonnablement complexe sous réserve que le traitement reste autonome. Elle se complexifie dès lors que les données proviennent d'un autre traitement et pour certaines, peuvent être transmises à un traitement tiers.

[9] Cf. Instruction ARM/SGA/DAJ/D2P relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense et au guide du responsable de traitement
[10] Création de fiches de traitement dans Sicl@de
[11] Depuis l'entrée en vigueur de la loi de 2018 il n'est plus besoin de déclaration préalable à l'ouverture d'un traitement. L'AIPD est obligatoire lorsqu'au moins 2 des critères suivants sont réunis :

- Évaluation/scoring (y compris le profilage) ;
- Décision automatique avec effet légal ou similaire ;
- Surveillance systématique ;
- Collecte de données sensibles ;
- Collecte de données personnelles à large échelle ;
- Croisement de données ;
- Usage innovant (utilisation d'une nouvelle technologie) ;
- Exclusion du bénéfice d'un droit/contrat ;
- Personnes vulnérables.

### C. L'élaboration de l'encadrement règlementaire du partage de la donnée par l'API-RH de SourceWeb

L'API est la réponse technique au partage de la donnée. Cette interface informatique permet aux solutions logicielles d'interagir entre elles de façon sécurisée. Elle facilite l'exécution de transactions et la transmission de données entre systèmes tiers.

Toutefois, en vertu du **principe de minimisation des données**, l'un des 6 principes fondamentaux légitimant un traitement de données, le RT est tenu à ne collecter que les données strictement nécessaires à la finalité du traitement.

Comment donc allier cet impératif règlementaire de proportionnalité avec l'ambition d'une interface d'être l'API-RH du ministère en transmettant des données issues de SIRH à des systèmes d'information clients dont la finalité n'est pas encore arrêtée dans le meilleur des cas, voire n'existent encore qu'à l'état d'idée ? Comment, alors que cette interface ne porte d'autre fonctionnalité métier que la dématérialisation du dossier de demande de pension, justifier de traiter l'intégralité des données présentes dans les SIRH, fournisseurs de ressources ?

C'est ce dilemme auquel a été confrontée l'interface SourceWeb[12] ouvrant ainsi la voie aux autres futures API et au dossier numérique de l'agent du ministère.

En étroite collaboration avec la Direction des affaires juridiques (DAJ) du ministère, désignée DPD, une ligne de conduite est définie concernant le renseignement de l'AIPD et un corpus règlementaire encadre dorénavant l'ouverture de l'API-RH SourceWeb au bénéfice d'applications clientes.

Ainsi, il est admis que l'AIPD est un document vivant et sa mise à jour est continue. Projet développé en mode agile, SourceWeb embarquera par vagues successives de plus en plus de données au gré des besoins matures des futures applications clientes. L'AIPD reflètera en conséquence ces enrichissements en agglomérant aux précédentes ces nouvelles données personnelles ainsi que la ou les nouvelles applications destinataires.

En revanche, les applications clientes de l'API-RH ne pourront à leur tour retransmettre les données issues de cette API-RH à un autre système d'information : la transmission par rebond de données issues d'une API est proscrite.

« Enfin, l'équipe projet et le DPD ont collaboré pour arrêter un corpus règlementaire dans le but de tracer et sécuriser la transmission des données vers les futures applications clientes ». Préalablement au déploiement de l'interface SourceWeb divers documents sont requis. Un contrat d'interface lie SourceWeb et les systèmes d'information de ressources humaines (SIRH), fournisseurs de ressources. Outre une homologation de sécurité[13], un arrêté portant création d'un traitement automatisé de données à caractère personnel est également publié et l'AIPD signée du RT, en l'occurrence le DRH-MD, est transmise à la CNIL.

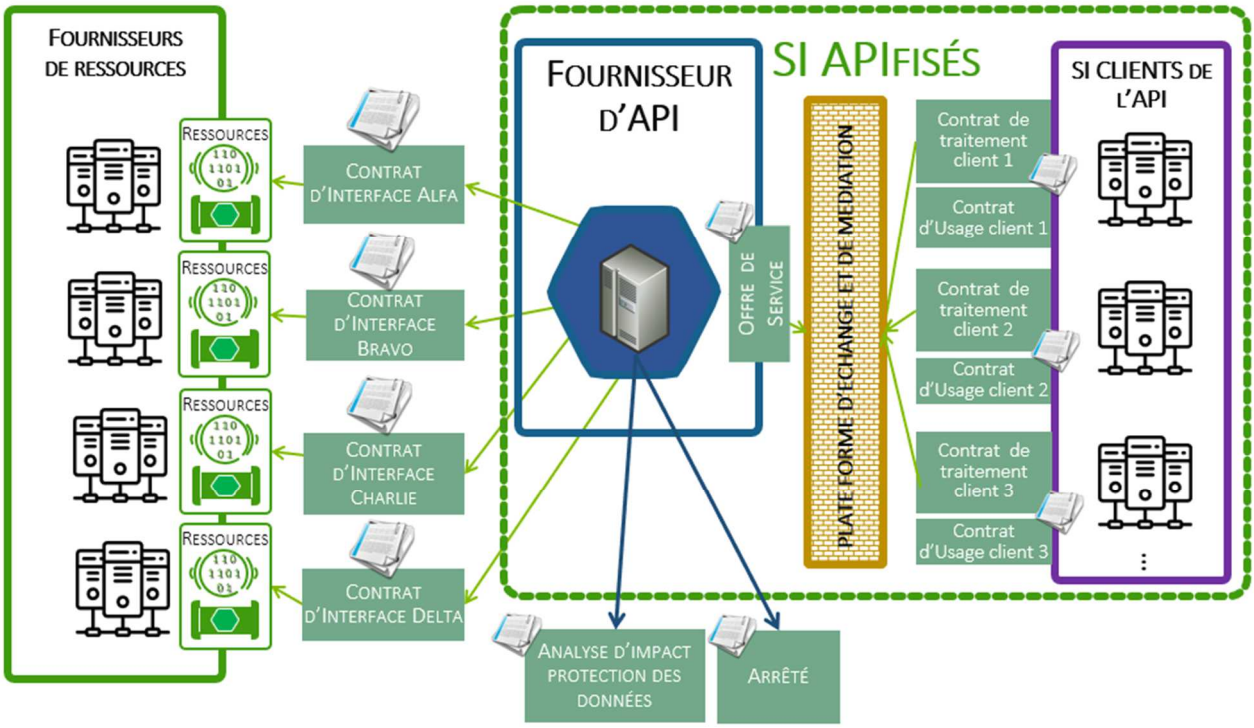
Concernant particulièrement l'API-RH, le ministère des Armées a fait le choix d'uniformiser le mode de présentation des API par le biais d'une plateforme d'échange et de médiation (PEM).

---

[12] L'interface SourceWeb, opérationnelle depuis juillet 2020, est devenue progressivement l'outil unique sur lequel est constitué le dossier dématérialisé de demande de pension des agents du ministère, réduisant ainsi considérablement le temps de traitement de ces dossiers

[13] Cf. Directive n° 27/ARM/DGNUM du 19 novembre 2019 portant sur l'homologation des systèmes d'information du ministère des armées

L'ouverture d'une API-RH suppose que le fournisseur d'API énonce à ses potentiels clients, dans une offre de services publiée sur la PEM, les services et données qu'il propose et surtout encadre leurs conditions d'utilisation. Le client quant à lui, outre sa propre AIPD, doit remettre au fournisseur un contrat d'usage qui comprend en annexe un contrat dit « de traitement » qui explique quelles données il souhaite consommer et les conditions de leur utilisation. C'est ce contrat d'usage qui permet d'ouvrir les services de l'API aux SI clients même en cas d'AIPD en cours de finalisation.




Le contrat d'usage est la pièce maîtresse du corpus règlementaire : il est le garant du respect du principe de minimisation des données partagées et du bon usage des API dans l'écosystème RH.

*
*  *

**En définitive**, cette réponse juridique au besoin d'agilité de projets informatiques qui se bâtissent incrémentalement peut paraître ardue mais elle accompagne favorablement la transformation numérique des ressources humaines en bordant le partage de la donnée dans la lettre et l'esprit de la règlementation relative à la protection des données personnelles.