Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2022

ÉPREUVE DE PROJET OU D'ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription.

Durée : 4 heures
Coefficient : 5

SPÉCIALITÉ : INFORMATIQUE ET SYSTEMES D'INFORMATION

OPTION : SYSTEMES D'INFORMATION ET DE COMMUNICATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 58 pages dont 1 annexe.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Vous êtes ingénieur territorial au sein de la Direction des Systèmes d'Information et des Services Numériques (DSISN) du conseil départemental d'INGEDEP (500 000 habitants). La crise sanitaire a eu l'effet d'un accélérateur dans les usages numériques de la collectivité qui a dû s'adapter en instaurant le télétravail, en accélérant les projets de dématérialisation et notamment la mise en place de la signature électronique. Ainsi, les accès à internet et les usages, de la part de tous, ont considérablement augmenté. En même temps, le constat d'une fracture numérique s'est confirmé pour les usagers mais aussi pour les agents d'INGEDEP.

Fort de ce constat, le directeur de la DSISN juge nécessaire d'élaborer un Plan de Transformation Numérique tourné à la fois vers les usagers et les agents d'INGEDEP.

Question 1 (4 points)

Vous rédigerez une note à l'attention du président d'INGEDEP dans laquelle vous définirez les grandes orientations stratégiques ainsi que quelques actions majeures devant être engagées au sein d'INGEDEP dans le cadre de cette transformation numérique.

Question 2 (6 points)

La sécurité et la conformité font partie des enjeux prioritaires de ce plan afin d'intégrer très en amont des projets toutes les problématiques de sécurité et de protection des données.

Vous citerez :

a) Les principales menaces, leurs sources ainsi que le contexte réglementaire, puis, les démarches à engager et la méthode à appliquer pour parvenir à réduire les risques de sécurité et garantir un niveau de conformité. (4 points)

b) Enfin, vous proposerez des actions auprès des agents pour les sensibiliser et les impliquer dans la sécurisation du système d'information d'INGEDEP. (2 points)

Question 3 (6 points)

Dans le cadre de la mise en œuvre des projets de ce Plan de Transformation Numérique, la direction générale d'INGEDEP vous demande qu'un travail de co-construction avec les Directions métiers soit engagé selon une méthodologie favorisant davantage la flexibilité, la souplesse, l'itération sur des temps plus courts.

a) Vous détaillerez dans un premier temps le renforcement de la dématérialisation et son impact auprès des usagers, des directions métiers, des agents ainsi que sur le système d'information. (4 points)

b) Vous proposerez et décrirez une méthodologie de projet ainsi qu'une organisation qui répondent à ces objectifs dans la réalisation et le suivi de ces projets du Plan de Transformation Numérique. (2 points)

Question 4 (4 points)

A l'instar de nombreuses collectivités, INGEDEP n'était pas totalement préparée à subir les conséquences de cette crise sanitaire et prend conscience de la dépendance de son fonctionnement au regard de la disponibilité et l'intégrité de son système d'information. Le recours à des solutions de type « cloud couputing » – ou informatique en nuage semble pouvoir permettre d'être réactif.

Néanmoins vous préciserez les questions que pose ce type de solution et les pistes de réflexions à prendre en compte en analysant leurs forces et faiblesses.

Liste des documents :

Document 1 : « Numérique : pourquoi il faut former les agents territoriaux » - *Lagazette.fr* - 15 juillet 2021 - 3 pages

Document 2 : « La signature électronique : un outil devenu incontournable » - *FranceNum.gouv.fr* - 7 décembre 2020 - 6 pages

Document 3 : « Protection de la vie privée dès la conception » - *Wikipédia* - 8 mars 2022 - 2 pages

Document 4 : « Règlement général sur la protection des données » (extrait) - *afcdp.net* - 2016 - 1 page

Document 5 : « Dématérialisation et inégalités d'accès aux services publics » - *defenseurdesdroits.fr* - 2019 - 10 pages

Document 6 : « Stratégie nationale pour le Cloud » - *France Relance* - 17 mai 2021 - 10 pages

Document 7 : « Bleu : renouveau ou mirage du cloud souverain 2.0 » - *lemondeinformatique.fr* - 31 mai 2021 - 1 page

Document 8 : "Cloud public : l'Etat labellise, les collectivités s'interrogent" - *Lagazette.fr* - 3 juin 2021 - 2 pages

Document 9 : « Référentiel général de sécurité (extrait) - *Agence nationale de la sécurité des systèmes d'information* - 13 juin 2014 - 7 pages

Document 10 : « Méthode AGILE : définition, étapes et exemples » - *Everlaab* - 2022 - 6 pages

Document 11 : « BRM, la courroie de transmission entre la DSI et les métiers » - *blog-orsys.fr* - 10 février 2017- 3 pages

Document 12 : « Le RGS : une bonne opportunité pour faire de la sécurité au sein des collectivités locales » - *advens.fr* - Consulté le 4 février 2022 - 2 pages

Liste des annexes :

Annexe 1 : « Présentation générale du Système d'Information d'INGEDEP » - INGEDEP - Novembre 2021 - 1 page

Documents reproduits avec l'autorisation du C.F.C.

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet

DOCUMENT 1

« Numérique : pourquoi il faut former les agents territoriaux » - *Lagazette.fr* - 15 juillet 2021

Alors que la crise sanitaire a ramené au premier plan l'importance de penser aux personnes éloignées du numérique, il faut aussi penser à l'inclusion numérique en interne. Une récente étude à laquelle ont participé plus d'un millier d'agents territoriaux révèle que deux tiers des participants n'ont pas le bagage numérique suffisant pour être autonomes dans leur vie professionnelle.

Face aux ambitions du gouvernement de dématérialiser l'ensemble des services publics d'ici 2022, les administrations suivent-elles en termes de compétences numériques en interne, indispensables pour rendre le meilleur service aux usagers ? Du côté des collectivités, une montée en compétences des agents sur le numérique apparaît indispensable. C'est d'ailleurs l'une des revendications figurant dans le manifeste élaboré à l'occasion du forum des Interconnectés, qui s'est déroulé les 17 et 18 mars.

La nécessité de former l'ensemble des agents

Lors de la session « accompagner les agents territoriaux » qui s'est déroulée le 17 mars, les Interconnectés et le groupement d'intérêt public PIX ont détaillé les résultats d'une étude inédite, menée avec le Syntec Numérique sur les compétences numériques des agents, que nous avions présentée lors d'un webinaire dédié, le 11 mars dernier.

1337 répondants ont participé à l'enquête avec des mises en situations concrètes pour évaluer leur niveau sur des actions comme la maîtrise de fichiers, de ses mails, les pratiques collaboratives, les réseaux sociaux, la sécurisation de son mot de passe, la maîtrise des données personnelles, le numérique responsable… Trois types de profils se dégagent : un niveau débutant, intermédiaire ou avancé.

Du fait des conditions de réalisation de l'enquête, et de la surreprésentation des filières administratives, des agents de catégorie A, et d'un échantillon un peu plus jeune, Marie Bancal, responsable du développement et des partenariats chez PIX souligne qu'il y a une « surreprésentation des personnes ayant une appétence pour le numérique, avec des résultats peut-être plus optimistes que la réalité ». Et pourtant, les voyants sont loin d'être dans le vert.

Un quart des répondants en grande difficulté sur le numérique

« Seules 35% des personnes sont autonomes, 38% ont un niveau intermédiaire et 27% sont débutants. Deux tiers des participants n'ont pas le bagage suffisant pour être en maîtrise de l'ensemble des situations professionnelles, sur un poste ayant une dimension numérique », a souligné Céline Colucci, déléguée générale des Interconnectés.

Au total, un quart des participants sont en grande difficulté, le manque de maîtrise de compétences numériques pouvant constituer une difficulté dans leur quotidien et être un frein à leur employabilité. Dans le chat, un participant abondait avec ces chiffres et indiquait

que « le manque de compétences numériques génère aujourd'hui un stress numérique lors du travail à distance ».

Si le facteur âge joue globalement positivement sur les compétences, il y a néanmoins « un besoin de formation sur l'ensemble des catégories d'âges », insiste Céline Colucci. Car même les plus jeunes répondants sont en difficulté sur des sujets clés tels que la cybersécurité ou les données personnelles.

Cyberattaques : les collectivités de plus en plus transparentes

Parmi les agents qui ont un niveau plutôt intermédiaire, il existe un décalage entre la perception qu'ils se font de leurs compétences numériques et leurs compétences réelles : ils ont tendance à minorer leurs difficultés et surévaluer leurs compétences. « Ces personnes peuvent être à l'aise avec un outil ou une pratique professionnelle bien rodée mais, quand elles sortent de ces schémas, elles ont moins de facilités », relève Céline Colucci. En termes de catégories, les agents de catégorie C sont ceux qui ont rencontré le plus de difficultés (35% ont un niveau débutant) et qui ont un fort souhait de formation (52% d'entre eux).

Expérimentations

Parmi les différents retours d'expériences proposés le 17 mars, Erwan Le Luron, chef de projet numérique au Grand Lyon a pu apporter celui de sa collectivité qui a expérimenté la montée en compétences numériques de 80 agents avec l'outil de microlearning Tiny Coaching puis une certification PIX, validée par 52 d'entre eux.

Béatrice Carpy, chargée de mission cité intelligente à Montpellier Méditerranée métropole, est revenue sur l'engagement des collectivités (la métropole, la ville, les CCAS) dans un processus de transformation numérique et d'accompagnement des agents avec l'outil PIX. « L'objectif est d'amener chaque agent à acquérir et développer des compétences numériques (…), et de proposer un passeport pour se débrouiller dans tous les champs de sa vie, professionnelle et personnelle, et faire valoir ses droits », a-t-elle détaillé.

Une offre PIX dédiée aux collectivités

PIX va désormais aller encore plus loin. Après des annonces concernant le secteur de la médiation numérique qui ont eu lieu en début de semaine, la banque des territoires et PIX ont annoncé mercredi 17 mars le développement d'une offre spécifique pour les collectivités, PIX PRO, afin d'accompagner la montée en compétences des agents en adéquation avec les métiers et les besoins spécifiques. Les collectivités désireuses de participer en mode test peuvent le faire sur le site Idealco.

Discussions en cours

La question de l'inclusion numérique en interne, et donc de la formation des agents, est en effet centrale. Le manifeste « pour des territoires numériques responsables », élaboré à l'occasion du forum et remis le 18 mars au gouvernement comporte d'ailleurs un passage dédié à la question de la montée en compétences numériques de l'ensemble des agents.

Cédric O, le secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques, a de nouveau rappelé, comme en début de semaine, que des enveloppes pouvaient être mobilisées pour la formation au numérique dans le cadre du plan de relance, et réaffirmé que ces questions faisaient l'objet de discussions avec l'AMRF concernant la formation des secrétaires de mairie, et avec le CNFPT concernant la formation plus large des agents territoriaux.

DOCUMENT 2
« La signature électronique : un outil devenu incontournable » - *FranceNum.gouv.fr* - 7 décembre 2020

La crise sanitaire a eu comme conséquence la limitation de nos déplacements et la généralisation du télétravail. La faculté de signer à distance est devenue indispensable pour continuer à réaliser les actes administratifs ou commerciaux, et permettre à l'entreprise de fonctionner.

Selon une enquête sur l'évolution des usages de la signature électronique en France, réalisée en janvier 2021 par YouGov pour Universign, 26 % des entreprises ont adopté une solution de signature électronique depuis le début de la crise sanitaire. Parmi elles, 49 % l'ont utilisée pour parapher des document réalisés dans le cadre de ventes et 41 % pour des documents liés aux ressources humaines.

Mais cet effort de numérisation apparait, d'après les répondants, inégal selon la taille des entreprises considérées : 41 % sont des PME, 53 % des ETI, et seulement 25 % des TPE. Pourtant les solutions de signature électroniques sont simples à mettre en œuvre et leur coût est très raisonnable.

Qu'est-ce que la signature électronique ?

La signature électronique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. Elle a **la même valeur légale qu'une signature manuscrite**. Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères.

A l'inverse, la signature numérique (dessiné par le signataire ou l'insertion d'une image) et la signature scannée n'ont pas la même force probante, elle ne permet pas de rapporter la preuve du consentement.

L'objectif majeur de la signature électronique est double :

- **garantir l'intégrité d'un document**, c'est-à-dire s'assurer que le document n'a pas été altéré entre sa signature et sa consultation ;
- **authentifier son auteur**, c'est-à-dire s'assurer de l'identité de la personne signataire ;
- **rapporter la preuve du consentement**.

Pour cela, elle doit avoir les **caractéristiques** suivantes :

- **authentique** : l'identité du signataire doit pouvoir être retrouvée de manière certaine
- **infalsifiable** : une personne ne peut pas se faire passer pour un autre
- **non réutilisable** : la signature fait partie du document signé et ne peut être déplacée sur un autre document
- **inaltérable** : une fois que le document est signé, on ne peut plus le modifier
- **irrévocable** : la personne qui a signé ne peut le contester

La signature électronique permet de signer en quelques secondes et sans contact physique des documents essentiels au bon fonctionnement des entreprises, tels que :

- les contrats de travail
- les factures

- les bons de commande
- les mandats et les compromis de vente
- les devis
- les documents comptables
- les documents juridiques
- les actes notariés

Quels sont les avantages de la signature électronique ?

La signature électronique, en permettant des gains temps et d'argent, est un outil au service de la productivité, tant pour l'expéditeur que pour le destinataire. Elle contribue à :

- **Faciliter l'envoi et l'échange des documents**, qui peuvent se faire, par un ordinateur ou un smartphone ;
- **Accélérer la procédure de signature** : les documents peuvent être signés en quelques secondes. Ils peuvent être aussi parafés simultanément par les parties, plutôt que successivement comme c'est le cas pour le papier ;
- **Suivre en temps réel l'avancement des dossiers** : on peut voir qui a signé et si besoin relancer, ceux qui n'ont pas encore signé ;
- **Sécuriser les données dématérialisées** : le tiers de confiance est garant de l'intégrité de vos données
- **Faire des économies** sur l'achat de papier, d'encre et d'impression des documents à signer ainsi que sur les frais d'envoi ou, le cas échéant de déplacement ;
- **Automatiser vos processus :** des traitements ou des actions peuvent être lancées une fois le document signé ;
- **Améliorer les conditions de vie de vos salariés et clients**, en leur permettant d'utiliser la signature électronique pour gérer leurs démarches administratives courantes, vous leur libèrerez du temps et contribuez à leur satisfaction globale.

Intégrer la signature électronique dans votre organisation c'est un premier pas dans votre transformation numérique. Elle constitue une vraie opportunité de repenser certains aspects du fonctionnement de votre entreprise. La grande majorité des logiciels de signature électronique offre des possibilités d'intégration à vos outils existants. Les outils numériques invitent en effet à de nouveaux modes de travail au service de vos clients et de votre stratégie. Cela participe à l'amélioration de votre image auprès de vos clients et vous permet de vous démarquer de vos concurrents.

Quelle est sa valeur juridique ?

Selon l'article 1366 du Code civil : *« L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »*

La signature électronique a la même valeur qu'une signature manuscrite en France comme dans le reste de l'Union européenne, depuis l'année 2000. Toutefois, ainsi que le précise le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique seule la **signature électronique qualifiée** est l'équivalent d'une signature manuscrite. Dans le cadre de la commande publique, une signature électronique avancée répond à ces conditions.

Standard européen depuis le 1er juillet 2016, l'eIDAS a fourni un cadre légal et pratique à son utilisation et a également harmonisé les règles régissant les signatures à l'échelle de toute l'Union européenne.

Ce règlement européen définit trois niveaux de sécurité : standard, avancé et qualifié. Les niveaux " avancé " et " qualifié ", qui font intervenir un tiers de confiance (le prestataire de la solution de signature électronique), sont les plus recommandés pour les entreprises. Ils sont parfaitement fiables devant les tribunaux, parce qu'ils garantissent l'identité des signataires d'un document, tout en respectant la Règlementation Européenne sur la Protection des Données (RGPD).

Quel type de signature électronique utiliser ?

Le choix du niveau de signature, tel que défini par l'eIDAS, dépend de l'usage, et de l'enjeu du document à signer : en cas de litige, plus votre signature aura un niveau de fiabilité fort, plus il sera difficile de contester la validité de l'acte signé et les engagements qu'il contient. Selon les cas on choisira le niveau de sécurité adapté.

La signature électronique standard (niveau 1)

La signature électronique manuscrite est utilisée par exemple lorsque vous tapez le code secret d'une carte de crédit, quand vous faites une signature manuscrite sur un appareil électronique, ou encore quand vous scannez une signature manuscrite, que vous apposez sur un document pour l'envoyer par mail. Elle est parfois appelée une signature numérique.
Sa valeur juridique est limitée, car elle ne garantit pas l'intégrité des données signées ni l'identité du signataire, etc. Elle peut toutefois valoir commencement de preuve par écrit. Sa vocation est de **simplifier des processus internes** où la signature est indispensable (autorisations, accusés de réception, commandes, contrats, etc.).

La signature électronique avancée (niveau 2)

C'est **la plus couramment utilisée par les entreprises**. Grâce à l'utilisation d'une clé privée accessible seulement à la personne qui signe et seulement à elle (son smartphone par exemple), elle permet :

- d'identifier la ou le signataire
- de lier la signature à son auteur
- de garantir l'intégrité de l'acte signé.

Concrètement, le signataire télécharge sa pièce d'identité sur la plateforme du prestataire de signature électronique qui peut ainsi procéder à des contrôles et l'authentifier.

Dans la pratique, c'est la signature électronique avancée, qui est la plus couramment utilisée. Ce type de signature est par exemple beaucoup utilisé pour signer une facture dématérialisée, un contrat de travail, un compromis de vente immobilier ou un contrat d'assurance vie. Elle nécessite toutefois l'acquisition d'un certificat de signature électronique répondant aux exigences de la norme eIDAS.

La signature électronique qualifiée (niveau 3)

Elle est la signature **la plus robuste sur les plans technique et juridique**. Ce type de signature exige que :

- l'identité du signataire soit validée en amont (en physique ou à distance selon certaines conditions), et ce par une autorité de certification ou un prestataire de service de certification électronique ;

- une clé de signature, un dispositif qualifié de création de signature électronique. Ce token physique (clé USB, carte à puce…), est délivré à uniquement à une personne physique. Une entreprise ne peut signer qu'au travers d'un représentant, une personne physique, dûment habilitée.

Selon le code civil, **seule cette signature est l'équivalent de la signature manuscrite**.

Plus lourde à mettre en œuvre et plus onéreuse, la signature qualifiée est généralement **réservée aux documents pour lesquels l'authentification est fondamentale**, par exemple, dans le cas de production d'actes notariés (notaires, huissiers…) ou dans le contexte des marchés publics (de l'appel d'offre à la facture).

Elle nécessite l'acquisition d'un certificat de signature électronique et un dispositif de création de signature électronique.

En pratique, comment fonctionne la signature électronique avancée (niveau 2) ?

Pour signer numériquement un contrat de location ou même un achat immobilier et que cela ait une valeur légale, il faut passer par un tiers de confiance. Ces entreprises habilitées à effectuer des opérations de sécurité juridique d'authentification, de transmission et de stockage sont nombreuses. Si elles proposent chacune leur solution, plus ou moins élaborées ou faciles d'utilisation, leur fonctionnement est relativement similaire : la procédure ressemble un peu à un achat en ligne, avec une authentification par code secret via SMS. Le processus est le suivant.

- Vous vous connectez sur le site du tiers de confiance en ligne à l'aide de vos identifiants, voire de votre clef électronique dans le cas d'une authentification qualifiée (niveau 3)

- Vous ajoutez les documents (word, PDF, etc…) que vous souhaitez faire signer.

- Vous invitez des signataires après avoir renseigné leurs coordonnées (en particulier leur numéro de téléphone portable).

- Chaque signataire reçoit par mail une notification pour signer ainsi qu'un code par SMS permettant de sécuriser la signature.

Quelques solutions numériques pour signer numériquement

Il existe de nombreux outils proposant la signature électronique et la gestion des transactions numériques

.

Les solutions de signature électronique proposées par les activateurs France Num

Sell&Sign est activateur France Num. Cette solution française de signature électronique propose une offre d'entrée, destinée aux TPE, à partir de 9,90 € HT par mois pour 5 signature (et 1,99 HT par signature supplémentaire). Des offres plus complètes sont accessibles sur devis. Sell&Sign propose aussi l'intégration de sa solution dans les solutions utilisées par ses clients.

L'américain Docusign est un des outils de e-signature les plus populaires. Il est également facile à prendre en main tout en proposant de nombreuses possibilités de personnalisation. Également certifié par l'ANSSI pour la signature de niveau 3, il a été choisi par les études notariales. Son offre de base propose pour 9 euros mensuels, la possibilité d'envoyer 5 documents par mois. Son offre standard permet à un utilisateur de signer et faire signer un nombre illimité de documents.

La solution de signature électronique du français LiveConsent propose un accès basique à partir de 7 euros par mois. Comptez 19 euros pour la version complète. L'interface, simple, est facile d'utilisation. Une API permet de lier la solution à votre site internet, vos applications ou vos logiciels (par exemple pour vos devis et factures).

Autres solutions de signature électronique

Yousign est une solution française facile d'utilisation. Ses tarifs de base sont très abordables. Sa solution nommée « One », propose les fonctionnalités essentielles de la signature électronique. Les tarifs vont de 9 €/mois pour un abonnement de 12 mois à 11 €/mois sans abonnement (activation et désactivation en un clic depuis l'appli).

Eversign propose à peu près les mêmes fonctionnalités que les précédents. Il peut s'intégrer à de nombreuses applications externes (Dropbox, Google Drive…), le tout avec un haut niveau de sécurité. Un bémol : il n'y a pas d'interface en français. La solution autrichienne offre une formule gratuite permettant de faire signer 5 documents par mois. Comptez 10 euros par mois et par utilisateur pour l'offre de base qui donne néanmoins accès à un nombre de documents illimité.

UniverSign, est un outil français, qui se distingue principalement par son mode de facturation à la carte, sous forme de crédits à consommer à la demande, sans engagement mensuel, de 49 euros HT pour 25 signatures, à 899 euros HT pour 500 signatures.

Signer en ligne, développé par Maileva / Docaposte, société du Groupe La Poste, propose une solution à partir de 49 euros par mois pour 3 utilisateurs avec une facturation additionnelle par circuit de signature comprise entre 1,20 et 1,45 euro par circuit, en fonction du nombre de circuits pré-acheté.

Docage, est une autre solution française très complète en terme de fonctionnalités. Elle permet notamment de créer des formulaires destinés à vos clients leur permettant de renseigner les informations qui seront insérées automatiquement dans le document à signer. Les tarifs sont

abordables : un abonnement de 4,9 € hors taxe par utilisateur et un coût de transaction de 0,75 € pour 1 signataire + 0,50 € par signataire supplémentaire.

Connective, entreprise belge, propose des signatures électroniques standards, avancées et qualifiées. Sa principale originalité c'est le fait d'intégrer des solutions d'identifications tierce pour faciliter et améliorer l'identification des signataires, dont France Connect. Utilisé par 20 millions de français, France Connect sécurise et simplifie la connexion à plus de 700 services en ligne proposée par l'État.

SignRequest, société néerlandaise, commercialise une solution de signature électronique pouvant s'intégrer à des logiciels pour les entreprises tels que Salesforce, Google Drive, Zapier ou encore Dropbox. Elle propose une offre gratuite permettant de signer 10 documents par mois et des offres comprises entre 7 et 12 euros par mois pour un nombre illimité de documents.

Focus sur l'archivage de vos documents signés électroniquement

Les entreprises ont des obligations de conservation de leurs documents, qu'ils soient au format papier ou électronique. Les documents qui sont signés ont en général une valeur légale importante. Leur archivage est donc primordial, par exemple pour pouvoir être produits en cas de futur litige avec un fournisseur. Les règles d'archivage des documents d'entreprise sont fixées soit par la loi, soit par les délais de prescription avant lesquels des contrôles peuvent être réalisés.

Les documents électroniques doivent être archivés dans des conditions de nature à garantir leur intégrité, de façon à s'assurer qu'ils ne puissent pas être altérés. Les éléments justifiant la validité de la signature électronique participent à sa fiabilité. Il faut donc conserver les éléments ayant servi à la conclusion de l'opération, appelés le « fichier de preuve » (certificats de signature des parties, preuve des processus mis en œuvre, horodatage etc.).

C'est pourquoi la plupart des prestataires de signature électronique proposent, en option ou par défaut, un archivage électronique des documents signés. La durée de conservation est en général fixée par défaut à 10 ans, avec la possibilité (payante) de la prolonger. Le problème c'est que cette durée standard de 10 années ne correspond souvent pas aux obligations réelles des entreprises. Par exemple, une durée de conservation de 10 ans à compter de la fin d'exécution du contrat n'a rien à voir avec une durée de 10 ans à compter de la signature du contrat !

Dans ces conditions, il est souvent préférable, au moins pour les documents dont la conservation est la plus longue, de prévoir leur récupération dans votre système d'archivage électronique des documents ou sur vos serveurs.

DOCUMENT 3

Protection de la vie privée dès la conception

La **protection de la vie privée dès la conception**, *privacy by design* en anglais, est une approche de l'ingénierie des systèmes qui prend en compte la vie privée tout au long du processus. Ce concept est un exemple de la *Value sensitive design* **(en)** (approche qui intègre les valeurs de l'humain dans tout le processus de la conception de la technologie). Ce concept découle d'un rapport de 1995 sur les technologies améliorant la confidentialité (outils et applications intégrés aux services et plateforme en ligne qui permettent de protéger les données personnelles) d'une équipe jointe composée de la Commissaire à l'Information et la Vie Privée de l'Ontario (Canada), Ann Cavoukian **(en)**, de l'Autorité de protection des données néerlandaise et de l'Organisation néerlandaise pour la recherche scientifique appliquée.

Principes fondamentaux

La protection de la vie privée dès la conception concerne l'imbrication de contrôles de protection des données dans les systèmes qui traitent des données personnelles à toutes les étapes de leur développement, incluant l'analyse, le design, la mise en œuvre, la vérification, la sortie, la maintenance et la mise hors service. Cela inclut les technologies améliorant la confidentialité qui pourraient réduire l'identifiabilité des données personnelles, telles que l'encodage ou la désidentification. Cela inclut aussi d'autres mesures telles que : donner le contrôle à l'utilisateur final en développant des mécanismes de consentement granulaire, mettre en œuvre des capacités de portabilité des données ou en développant des mises en garde sur la vie privée plus facilement compréhensibles. La façon dont la protection de la vie privée dès la conception (*Privacy by Design*) ou l'intégration de la sécurité dès la conception (Security by Design **(en)**) est faite dépend de l'application, des technologies et du choix d'approche. Cependant, plusieurs normes et conseils sont disponibles ou en cours d'élaboration.

Le Privacy by Design repose sur 7 principes fondamentaux développés par Ann Cavoukian **(en)**, basés sur les 7 "Lois de l'identité" (7 *"Laws of Identity"*) de Kim Cameron[1] :

1. Prendre des mesures proactives et non réactives, des mesures préventives et non correctives (prévoir et de prévenir les incidents liés à l'atteinte de la vie privée avant même qu'ils ne se produisent)
2. Assurer la protection implicite de la vie privée (faire en sorte que les données personnelles soient protégées de manière automatique avec un paramétrage par défaut des nouvelles technologies assurant un niveau de protection maximum des données sans que l'utilisateur ait à définir de paramètres spécifiques)
3. Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques
4. Assurer une fonctionnalité complète selon un paradigme à somme positive et non à somme nulle (assurer la protection de la vie privée sans nuire à la mise en œuvre d'autres fonctionnalités)
5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
6. Assurer la visibilité et la transparence (chaque élément intégré aux systèmes lié à la protection des données personnelles doit rester visible et transparent en cas de vérification indépendante)
7. Respecter la vie privée des utilisateurs

Adoption mondiale du concept

Dès 1997, l'Allemagne a adopté une loi (§ 3 IV TDDG) sur la sécurité et l'information qui réglemente, entre autres la protection de la vie privée. En octobre 2010, des régulateurs du monde entier se sont réunis à l'assemblée annuelle de l'International Data Protection and Privacy Commissioners de Jérusalem, Israël. Ceux-ci ont unanimement pris la résolution reconnaissant la protection de la vie privée dès la conception comme une composante essentielle de la protection fondamentale de la vie privée. Cette décision a été suivie par la Commission fédérale du commerce des États-Unis qui a reconnu en 2012 le *Privacy by Design* comme l'une des trois pratiques recommandées pour protéger la vie privée en ligne dans un rapport intitulé *Protecting Consumer privacy in an Era of Rapid Change* (*Protection de la Vie privée du Consommateur dans un Contexte de Changement Rapide*)[2]. La protection des données dès la conception (*Data Protection by Design*) a été également incorporée dans les plans de la Commission européenne qui vise à unifier la protection des données dans l'Union Européenne sous une seule et même loi – le Règlement général sur la protection des données, ou la *General Data Protection Regulation*. Néanmoins, la dernière proposition ne donne aucun élément de définition de la protection des données dès la conception ni de la protection de la vie privée dès la conception. Ce qui est entendu par ces concepts reste flou. Des initiatives ont tenté de révéler ce problème telles que le projet OWASP des 10 principaux risques d'atteinte à la vie privée[3] : elles traitent d'applications en ligne et donnent des pistes sur la manière dont le Privacy by Design s'est intégré dans les pratiques. Le cœur du principe de technologie neutre du Règlement général sur la protection des données est qu'il dépend des fabricants de documenter la conformité, y compris le *Privacy by Design* selon le principe de « Si tu peux, tu dois. »

Critiques

Le privacy by design dans son sens fondamental a été critiqué comme étant trop « vague » et laissant plusieurs questions sans réponses concernant son application dans les systèmes d'ingénierie. Il a également été pointé du doigt le fait que le concept est similaire à celui de Voluntary compliance dans les industries qui impactent sur leur environnement. Qui plus est, l'approche évolutive qui est couramment adoptée pour développer le concept se fera au détriment des violations de la vie privée puisque l'évolution implique de laisser des phénotypes inadaptés (produits envahissant la vie privée) subsister tant qu'ils n'auront pas été clairement identifiés comme inadaptés pour la sauvegarde de la vie privée. De plus, certains business modèles sont développés sur la surveillance des utilisateurs et sur la manipulation de données ce qui entraîne que la conformité volontaire au concept est peu probable. Une autre critique repose sur le fait que les définitions courantes de le *Privacy by Design* n'abordent pas l'aspect méthodologique des systèmes d'ingénierie, par exemple l'utilisation de méthodes décentes d'ingénierie des systèmes qui couvre le système complet durant tout le cycle de vie des données. Par ailleurs, le concept ne se concentre pas sur le rôle du détenteur des données, mais plutôt sur le rôle du concepteur du système. Ce dernier rôle n'étant pas utilisé dans les lois sur la vie privée, le concept ne repose donc pas directement sur la loi. Depuis que le concept fait partie intégrante de recherches et de développements politiques, des biais peuvent survenir dans les définitions utilisées. Un exemple est la tendance dans la législation nord-américaine à laisser les entreprises elles-mêmes définir ce que le concept devrait désigner (approche évolutive), alors que l'Union européenne tend à adopter une approche plus réglementaire, bien que rien n'est encore été instancié.

Vers le *privacy by using*

Un des principes fondateurs du privacy by design est d'assurer une protection des individus, et ce sans actions préalables de leur part. Cependant, une restriction technique de la divulgation des données risquerait d'être inefficace, car s'appliquant à des acteurs qui n'en veulent pas. Il convient donc de promouvoir le concept de *privacy by using* parallèlement à celui de *privacy by design*. Celui-ci repose sur le développement d'instruments technologiques, juridiques et informationnels permettant de développer une capacité d'apprentissage chez l'individu. Il lui serait alors moins demandé d'agir que d'apprendre pour construire un comportement éclairé sur la base d'une meilleure connaissance de son environnement informationnel et des conséquences de ses comportements de divulgation (on parle d'*empowerment*). De ces comportements éclairés pourraient émerger de nouvelles normes de *privacy* [4].

CHAPITRE IV
Responsable du traitement et sous-traitant

Section 1
Obligations générales

Article 24
Responsabilité du responsable du traitement

1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

Considérant 76 : Il convient **de déterminer la probabilité et la gravité du risque** pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une **évaluation objective** permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé.

Considérant 77 : Des directives relatives à la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou le sous-traitant du respect du présent règlement, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque, pourraient être fournies notamment au moyen de **codes de conduite approuvés**, de certifications approuvées et de lignes directrices données par le comité ou d'indications données par un délégué à la protection des données. Le comité peut également publier des lignes directrices relatives aux opérations de traitement considérées comme étant peu susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et indiquer les mesures qui peuvent suffire dans de tels cas pour faire face à un tel risque.

Article 25
Protection des données dès la conception et protection des données par défaut

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

Considérant 78 : La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel exige l'adoption de mesures techniques et organisationnelles appropriées pour garantir que les exigences du présent règlement sont respectées. Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, **les principes de protection des données dès la conception et de protection des données par défaut**. Ces mesures pourraient consister, entre autres, à **réduire à un minimum le traitement des données** à caractère personnel, à **pseudonymiser les données** à caractère personnel dès que possible, à **garantir la transparence** en ce qui concerne les fonctions et le traitement des données à caractère personnel, à **permettre à la personne concernée de contrôler le traitement des données**, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer. Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données.Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics.

Article 26
Responsables conjoints du traitement

1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Considérant 79 : La protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et des sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par celles-ci, **exige une répartition claire des responsabilités** au titre du présent règlement, y compris lorsque le responsable du traitement détermine les finalités et les moyens du traitement conjointement avec d'autres responsables du traitement, ou lorsqu'une opération de traitement est effectuée pour le compte d'un responsable du traitement.

Introduction

En vertu de l'article 71-1 de la Constitution et de l'article 4 de la loi organique du 29 mars 2011, le Défenseur des droits veille au respect des droits et libertés par les administrations de l'Etat, les collectivités territoriales, les établissements publics, ainsi que par tout organisme investi d'une mission de service public ou à l'égard duquel la loi organique lui attribue des compétences.

Dans cette mission, le Défenseur des droits est souvent le dernier recours des usagers confrontés à des difficultés inextricables dans leurs relations avec les administrations. Cette responsabilité fait du Défenseur des droits un observateur privilégié des situations où les services publics ne respectent pas les droits et libertés des usagers. Si certaines de ces situations sont anciennes et récurrentes, sa mission lui permet d'identifier, d'analyser et de tenter de résoudre les difficultés émergentes.

Dès 2013 et l'annonce du « choc de simplification » des démarches administratives par le Gouvernement, la question de la numérisation des services publics a commencé à apparaître, à la lumière des réclamations qui nous étaient adressées, comme un sujet de préoccupation.

Trois ans plus tard, nous avons reçu plusieurs milliers de réclamations sur le seul sujet du processus de dématérialisation de la délivrance des permis de conduire et des certificats d'immatriculation mis en place dans le cadre du Plan préfectures nouvelle génération (PPNG), faisant de ce sujet un des premiers motifs de saisine de l'institution.

Au travers du programme de transformation de l'administration, lancé en octobre 2017 et baptisé « Action Publique 2022 », le Gouvernement souhaite améliorer la qualité de service pour les usagers en développant notamment la relation de confiance entre les usagers et les administrations. « Action Publique 2022 » repose sur six principes clés, dont celui de la priorité donnée à la transformation numérique des administrations, avec pour objectif la dématérialisation de l'intégralité des services publics à horizon 2022.

Cette ambition se justifie, par l'idée que la dématérialisation des procédures administratives permet de simplifier, pour une majorité d'usagers, l'accès aux informations ou aux documents administratifs. Elle permet également, dans certaines hypothèses, de lutter contre le non recours, et d'améliorer l'accès réel de certains usagers à leurs droits, tout en respectant mieux leur dignité. On pense ici aux interminables files d'attentes aux guichets de certains services publics, simplement pour obtenir un rendez-vous ou parfois, *in fine*, ne pas se voir délivrer le service en question pour des raisons parfois difficiles à comprendre pour l'usager, voire même pour des motifs dilatoires ou illégaux.

Compte tenu de la réflexion sur la simplification et la clarification des procédures administratives qu'elle peut entrainer, la dématérialisation peut constituer un puissant levier d'amélioration de l'accès de tous et de toutes à ses droits.

Mais cet objectif ne sera pas atteint si l'ambition collective portée dans ce processus se résume à pallier la disparition des services publics sur certains territoires et à privilégier une approche budgétaire et comptable. De même, si l'on considère que cette transformation profonde des relations entre usagers et services publics peut se faire à « marche forcée », sans tenir compte des difficultés bien réelles d'une partie de la population et des besoins spécifiques de certaines catégories d'usagers. Il ne sera pas plus atteint si cette évolution aboutit à une déresponsabilisation des pouvoirs publics, en renvoyant notamment à la sphère associative la prise en charge de l'accompagnement des usagers, ou en misant sur le secteur privé pour compenser les défaillances du service public.

Pour bénéficier à tous et à toutes, la dématérialisation des services publics devra constituer un investissement massif pour notre pays, pour l'Etat, bien sûr, mais également pour l'ensemble des acteurs du service public et pour les usagers qui devront s'y adapter. Les pouvoirs publics ne devront jamais perdre de vue que, dans cette transformation en profondeur de nos services publics, l'objectif premier devra rester l'amélioration du service rendu aux usagers, à tous les usagers, et le maintien des droits pour tous. Si une seule personne devait être privée de ses droits du fait de la dématérialisation d'un service public, ce serait un échec pour notre démocratie et pour l'Etat de droit.

Aucune organisation administrative, aucune évolution technologique ne peut être défendue si elle ne va pas dans le sens de l'amélioration des droits, pour tous et pour toutes. Comme le montre ce rapport, perdre le sens de cette transformation, ou sous-estimer ses effets, conduirait à priver de leurs droits certains et certaines d'entre nous, à exclure encore davantage de personnes déjà

exclues, à rendre encore plus invisibles ceux et celles que l'on ne souhaite pas voir. Nous serions alors exposés à un recul inédit de ce qu'est le service public en France et à une dégradation du respect des droits et libertés par les administrations et les organismes chargés d'une mission de service public.

Il faut ici réaffirmer ce qui semble ne plus être une évidence pour tous les responsables : un service public dématérialisé reste un service public avec tout ce que cela impose de contraintes pour respecter les droits de manière égale sur l'ensemble du territoire et pour toutes les catégories de population.

La mise en œuvre des politiques publiques de dématérialisation se doit donc de respecter les principes fondateurs du service public : l'adaptabilité, la continuité et l'égalité devant le service public.

- **Le principe de continuité du service public** : ce principe constitue un des aspects de la continuité de l'État et a été qualifié de principe de valeur constitutionnelle par le Conseil constitutionnel dans sa décision 79-105 DC du 25 juillet 1979. Il repose sur la nécessité de répondre aux besoins d'intérêt général sans interruption.
- **Le principe de l'égalité devant le service public** : corollaire du principe d'égalité devant la loi ou devant les charges publiques consacré par la Déclaration des droits de l'Homme et du citoyen du 27 août 1789, ce principe implique que les personnes se trouvant dans une situation identique à l'égard du service public doivent être régies par les mêmes règles.
- **Le principe d'adaptabilité ou de mutabilité** : à la lumière de ce principe, l'autorité administrative doit prendre les mesures d'adaptation du service public afin d'assurer un accès « normal » de l'usager au service public, et elle ne saurait adapter le service public avec pour conséquence que soit compromis cet accès « normal ».

Bien sûr, un déploiement harmonieux de la dématérialisation, qui soit respectueux des droits des usagers, voire qui en renforce l'effectivité, est possible mais à certaines conditions.

Dans le cadre de ses travaux, le Défenseur des droits a analysé les exemples tirés des situations qu'il a observées mettant en cause les processus de dématérialisation des services publics. En vue de compléter l'analyse des saisines adressées au Défenseur des droits, une série d'entretiens a été menée auprès de différents acteurs porteurs de réformes de dématérialisation, d'associations accompagnant les usagers dans les démarches administratives, d'associations d'élus, et de services ministériels. L'ensemble des personnes et institutions qui ont nourri ces réflexions sont ici remerciés.

Le présent rapport entend donc, à partir d'exemples concrets, alerter sur les risques et dérives de la transformation numérique des services publics. Mais il entend également contribuer, au travers de nombreuses recommandations, à faire en sorte que ce processus inéluctable, et fondamentalement positif pour la qualité du service public, respecte les objectifs de services publics sans laisser personne de côté.

Synthèse des principales recommandations

Conserver toujours plusieurs modalités d'accès aux services publics

- Adopter une disposition législative au sein du code des relations entre les usagers et l'administration imposant de préserver plusieurs modalités d'accès aux services publics pour qu'aucune démarche administrative ne soit accessible uniquement par voie dématérialisée.

Prendre en compte les difficultés pour les usagers

- Créer une clause de protection des usagers en cas de problème technique leur permettant de ne pas être considérés comme responsables du non-aboutissement de la démarche.
- Instaurer le principe de l'envoi sous forme papier des notifications d'attribution, de suppression ou de révision de droits comportant des délais et des voies de recours, sauf si la personne consent expressément et au préalable aux échanges dématérialisés.
- Garantir un délai permettant de faire des rectifications dans le cadre d'une démarche administrative dématérialisée.
- Prévoir des exceptions juridiques aux obligations de paiement dématérialisé imposées par la réglementation, et que soit garanti, quelle que soit la procédure dématérialisée, l'existence d'une autre modalité de paiement que celles liées à la possession d'un compte bancaire.

Repérer et accompagner les personnes en difficulté avec le numérique

- Organiser un test d'évaluation des apprentissages fondamentaux de l'usage du numérique à l'occasion de la journée défense et citoyenneté.
- Evaluer systématiquement les besoins d'accompagnement liés aux projets de dématérialisation, prévoir les moyens dédiés et expliciter les mesures prises ou à prendre pour y faire face.
- Redéployer une partie des économies procurées par la dématérialisation des services publics vers la mise en place de dispositifs pérennes d'accompagnement des usagers.
- Instaurer un service public de proximité réunissant un représentant de chaque organisme social, des impôts, de pôle emploi, un travailleur social ainsi qu'un médiateur numérique pour réaliser un accompagnement généraliste et de qualité de la population, en particulier la plus fragile. L'échelon de mise en œuvre du nouveau dispositif pourrait être adapté en fonction des besoins des territoires.

Améliorer et simplifier les démarches dématérialisées pour les usagers

- Favoriser l'usage d'un identifiant unique pour accéder à l'ensemble des services publics dématérialisés.
- Améliorer l'information des usagers afin de faire mieux connaitre la gratuité des démarches administratives et mettre fin aux pratiques d'orientation des usagers vers un service privé payant.

Former les accompagnateurs

- Renforcer la formation initiale et continue des travailleurs sociaux et des agents d'accueil des services publics à l'usage numérique, à la détection des publics en difficulté et à leur accompagnement.
- Former les volontaires du service civique à l'accueil des publics fragiles et mobiliser ces volontaires non pour remplacer les agents d'accueil mais en complément de la mobilisation des agents de l'organisme qui dématérialise des procédures.

Prendre en compte les publics spécifiques

- Permettre à l'ensemble des personnes privées de leur liberté, en particulier dans les établissements pénitentiaires, de disposer d'un accès effectif aux sites internet des services publics, des organismes sociaux et aux sites de formation en ligne reconnus par le ministère de l'Education nationale.
- Généraliser rapidement le double accès aux comptes personnels à tous les sites des services publics, un pour le majeur protégé, un pour le mandataire judiciaire, adaptés à chaque mandat.
- Mettre en œuvre systématiquement des mesures appropriées afin de permettre aux personnes handicapées d'accéder effectivement à leurs droits en cas d'impossibilité avérée de mise en accessibilité d'un site internet existant et dans l'attente de la mise en place d'un site répondant aux normes d'accessibilité.

Le contexte du rapport

En vertu de l'article 71-1 de la Constitution et de l'article 4 de la loi organique du 29 mars 2011, le Défenseur des droits veille au respect des droits et libertés par les administrations de l'Etat, les collectivités territoriales, les établissements publics, ainsi que par tout organisme investi d'une mission de service public ou à l'égard duquel la loi organique lui attribue des compétences.

Dès 2013, et l'annonce du « choc de simplification » des démarches administratives souhaité par le gouvernement, la question de la numérisation des services publics a commencé à apparaître comme un sujet d'actualité et de préoccupations, nourries par les réclamations adressées à l'institution. D'ailleurs, depuis 2014, cette question de la dématérialisation figure dans tous les rapports annuels d'activité de l'institution et le Délégué général à la médiation avec les services publics, Bernard Dreyfus, a focalisé son propos sur la fracture numérique et le Plan préfecture nouvelle génération, dans le rapport d'activité de l'année 2017.

Depuis novembre 2017, plusieurs milliers de réclamations portant sur le seul sujet du processus de dématérialisation de la délivrance des permis de conduire et des certificats d'immatriculation mis en place dans le cadre du Plan préfectures nouvelle génération (PPNG) ont été reçues, faisant de ce sujet un des premiers motifs de saisine de l'institution. Outre ces saisines, d'autres difficultés liées à la dématérialisation des services publics, que ce soit pour les demandes de prestations sociales, les demandes de titres de séjour ou encore les déclarations de revenus, etc., ont été signalés à l'institution.

Observateur privilégié des effets de la dématérialisation des services publics, le Défenseur des droits a, en conséquence, décidé d'analyser en profondeur les exemples tirés de ces réclamations pour mieux identifier les situations de risque que ce processus de modernisation des services publics fait peser sur l'accès au(x) droit(s).

L'objectif de dématérialiser l'intégralité des services publics à l'horizon de 2022, dans le cadre du programme de transformation de l'administration « Action publique 2022 », lancé en octobre 2017, ne pourra être atteint si la dématérialisation se fait à « marche forcée », sans tenir compte des difficultés bien réelles d'une partie de la population et des besoins spécifiques de certaines catégories d'usagers. Les effets de la dématérialisation pourraient conduire à exclure encore davantage de personnes déjà exclues, à rendre encore plus invisible ceux et celles que l'on ne souhaite pas voir.

Ce qui serait un recul inédit de ce qu'est le service public en France.

Le présent rapport entend donc, à partir d'exemples concrets, alerter sur les risques et dérives que la transformation numérique des services publics induits. Il souhaite également, au travers de nombreuses recommandations, démontrer que ce processus, dès lors qu'il respecte les principes et les objectifs du service public, sans laisser personne de côté, peut être fondamentalement positif pour la qualité du service rendu aux usagers.

Si une seule personne devait être privée de ses droits du fait de la dématérialisation d'un service public, ce serait un échec pour notre démocratie et pour l'Etat de droit.

La dématérialisation : une source d'amélioration pour l'accès aux services publics ...

Au travers du programme de transformation de l'administration, lancé en octobre 2017 et baptisé « Action Publique 2022 », le gouvernement souhaite améliorer la qualité de service des services publics en développant notamment la relation de confiance entre les usagers et les administrations.

La possibilité de réaliser un certain nombre de démarches administratives en ligne, plutôt qu'au guichet ou par téléphone, représente non seulement une source d'économies pour l'administration, mais également une source de bénéfices pour les usagers. Cette transformation peut faciliter l'accès à l'information, constituer un progrès pour l'accès aux droits quand elle s'accompagne de démarches de simplification et d'automatisation et notamment favoriser la lutte contre le non recours.

Exemples

- la dématérialisation du revenu de solidarité active (RSA) a permis une hausse de 2% des bénéficiaires.
- la dématérialisation de la prime d'activité s'est révélée un facteur d'amélioration de l'accès à cette prestation avec un taux de recours élevée, estimé à 73% et dépassant ainsi de 23% les projections initiales.
- la création du « coffre-fort numérique » pour les personnes en situation de grande précarité.

Mais un risque potentiel d'exclusion pour l'ensemble des usagers des services publics

Les démarches administratives en ligne nécessitent a minima une connexion internet de qualité et l'accès à des équipements informatiques. Ces deux conditions, évidentes, ne sont pas réunies sur l'ensemble du territoire et dans l'ensemble des foyers français, créant des inégalités face aux possibilités d'usage des services publics en ligne, et, dans les cas où le seul moyen d'accès aux services est internet, une rupture d'égalité devant le service public.

Un risque de fracture territoriale

Pour les habitants des zones rurales, il existe un risque réel de fracture territoriale lié à l'existence de zones blanches et grises.

- 0, 7 % des français, soit 500.000 personnes, n'ont pas accès à une connexion internet fixe[2].
- Dans les communes de moins de 1000 habitants plus d'un tiers des habitants n'ont pas accès à un internet de qualité. Cela représente près de 75% des communes de France et 15% de la population.

L'accès au matériel informatique et à une connexion internet de qualité, reste difficile dans les territoires ultramarins. L'Outre-mer n'a pas bénéficié contrairement à la métropole du développement des offres de forfaits « low cost » et de la baisse des prix.

Une conception et un déploiement des sites internet parfois inadaptés

Des difficultés sont susceptibles d'empêcher les usagers d'accéder au service public dématérialisé comme des problèmes d'ergonomie des sites ne permettant pas aux usagers une navigation intuitive, ni de joindre des pièces au-delà d'une certaine taille, ou encore le sous dimensionnement des sites pour absorber le flux des demandes.

Le Défenseur des droits recommande de toujours conserver plusieurs modalités d'accès aux services publics. Aucune démarche administrative ne doit être accessible uniquement par voie dématérialisée.

L'accompagnement des usagers

De nombreuses personnes en difficulté face au numérique

Il est nécessaire que les personnes soient accompagnées dans l'usage du numérique pour éviter que la transformation numérique des services publics n'aggrave encore leurs difficultés. Cet accompagnement doit s'adapter aux différents publics, très hétérogènes, ainsi qu'aux multiples difficultés d'usage.

- En 2017, 12% de la population âgée de 12 ans et plus, soit près de 7 millions de personnes, ne se connectent jamais à internet et un tiers des Français s'estime peu ou pas compétent pour utiliser un ordinateur, soit 18 millions de personnes[3].
- La fracture numérique est également une fracture sociale et culturelle. Le taux de connexion à internet varie ainsi de 54% pour les non diplômés à 94% pour les diplômés de l'enseignement supérieur.

Si les moins de 18 ans sont majoritairement très à l'aise avec l'internet ludique, ils sont 17% à être en réelle difficulté pour les démarches administratives.

L'absence de connexion est très élevée chez les retraités, les non-diplômés et les personnes ayant de faibles revenus.

Pour être autonome, l'usager doit maîtriser l'usage d'internet dans sa globalité afin de saisir l'ensemble des informations correctement (créer une adresse mail, se souvenir des mots de passe, créer un espace personnel).

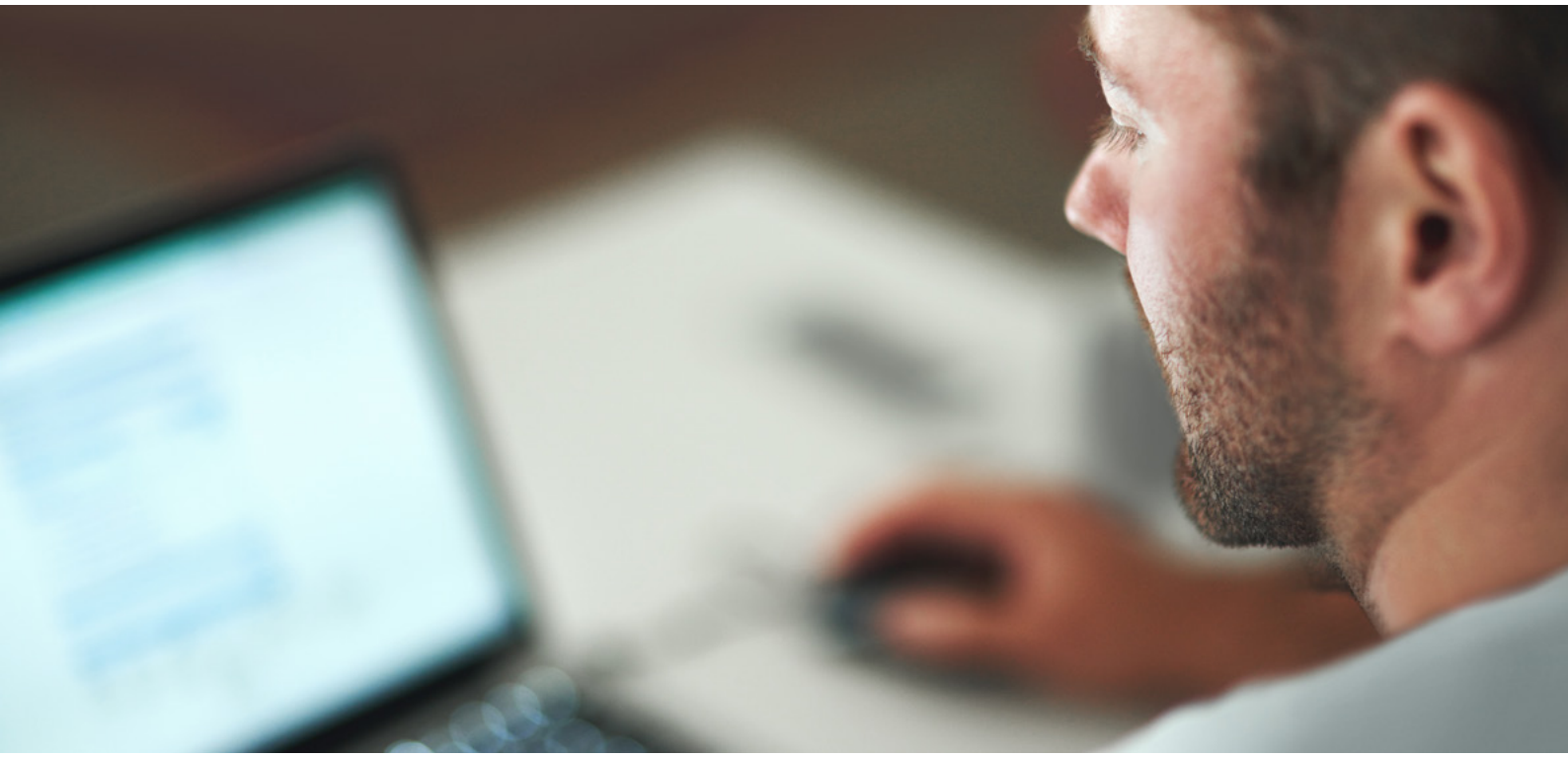
Les difficultés d'usage peuvent également entraîner des erreurs lors de la saisie des informations pour une demande, ou sur les cases à cocher. Les personnes peuvent faire un mauvais choix, ou une mauvaise manipulation ce qui peut entraîner une perte de leurs droits.

Une insuffisance dans l'accompagnement

Bien que des efforts ont été réalisés dans le but d'accompagner les usagers dans le processus de dématérialisation des services publics, avec la mise en place de « point numériques » ou de maisons de services au public, ils restent encore insuffisants par rapport au besoin d'accompagnement.

La dématérialisation des services publics ne doit pas être pensée indépendamment des autres canaux d'accès aux services publics. Il est donc nécessaire de repenser par exemple les services téléphoniques.

[2] Accès à l'internet fixe, fracture numérique inédite aujourd'hui, factures en hausse demain, Etude UFC Que Choisir, septembre 2017
[3] Chiffres CREDOC 2017 Baromètre numérique



Le Défenseur des droits considère que l'exclusion que peut entraîner la dématérialisation peut être combattue en donnant les moyens à chacun de devenir autonome face au numérique. C'est pourquoi le Défenseur des droits restera très attentif à la mise en œuvre des dispositifs dans le cadre du plan pour un numérique inclusif lancé par l'Etat.

Un transfert de charge vers les associations et le risque de basculement vers le secteur privé et payant

Le Défenseur des droits appelle l'attention des pouvoirs publics sur le fait que la dématérialisation des services publics n'est pas sans conséquences sur l'activité des acteurs du milieu associatif qui accompagne les personnes les plus fragiles. Ces acteurs doivent disposer d'un appui pour que l'accompagnement qu'ils sont obligés de réaliser du fait de la dématérialisation soit facilité et ne pèse pas outre mesure sur leurs missions premières.

Le Défenseur des droits constate que les usagers en difficulté ont régulièrement recours à des prestataires privés afin d'effectuer, moyennant rémunération, leurs démarches administratives dématérialisées. Or, les usagers n'ont pas toujours connaissance de la possibilité de réaliser gratuitement ces procédures via les sites publics, dont celui de l'ANTS, et se retrouvent donc à payer ces tiers pour réaliser une démarche en pensant que le paiement est obligatoire. Cette confusion entraîne également des risques d'escroquerie envers les usagers, qui pensent à tort recourir à des tiers labellisés.

Le Défenseur des droits souligne que plus la personne est en situation de vulnérabilité numérique ou administrative, plus elle est susceptible d'avoir recours à un tiers payant, ce qui représente un risque de rupture d'égalité devant le service public.

Le Défenseur des droits recommande :

- **de repérer et d'accompagner les personnes en difficulté avec le numérique en redéployant par exemple une partie des économies procurées par la dématérialisation des services publics vers la mise en place de dispositifs pérennes d'accompagnement des usagers ;**
- **de prendre en compte les difficultés pour les usagers en créant une clause de protection des usagers en cas de problème technique leur permettant de ne pas être considérés comme responsables du non-aboutissement de la démarche ;**
- **d'améliorer et simplifier les démarches dématérialisées pour les usagers en favorisant l'usage d'un identifiant unique pour accéder à l'ensemble des services publics dématérialisés et en informant mieux sur la gratuité des démarches administratives afin de mettre fin à l'orientation vers un service privé payant ;**
- **de renforcer la formation initiale et continue des travailleurs sociaux et des agents d'accueil des services publics à l'usage numérique, à la détection des publics en difficulté et à leur accompagnement.**

Porter une attention particulière aux « laissés pour compte » de la dématérialisation

Les personnes en situation de handicap

L'article 47 de la loi n°2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées, modifié notamment par la loi du 5 septembre 2018, introduit une obligation d'accessibilité des services de communication au public en ligne des « organismes du secteur public ».

Le Défenseur des droits constate, cependant, que le dispositif prévu par la loi est, à ce jour, peu contraignant, tant en termes d'obligation que de réalisation et de sanction et qu'il ne permet pas de garantir un accès effectif aux sites internet des services publics pour les personnes en situation de handicap, dans un contexte où certaines démarches administratives sont d'ores et déjà totalement dématérialisées ou en voie de l'être.

Malgré la mise en place du Référentiel Général d'Accessibilité pour les Administrations (RGAA) qui doit permettre aux personnes en situation de handicap de naviguer sur les sites administratifs en toute autonomie, le Défenseur des droits constate que la plupart des sites publics de l'État ne sont toujours pas en conformité avec la règlementation en vigueur. Ce qui induit une fracture supplémentaire en raison de l'inaccessibilité de ces sites.

Quant à la situation spécifique des majeurs protégés, le Défenseur des droits a pu constater qu'elle était rarement prise en compte dans le cadre de la dématérialisation des services publics. L'absence d'accès spécifique dédié au tuteur sur les sites de démarches en ligne contraint donc ce dernier à utiliser les identifiants personnels du majeur protégé et à l'exclure de fait de la démarche administrative et donc de ses droits fondamentaux.

Le Défenseur des droits recommande la généralisation rapide à tous les sites des services publics d'un double accès aux comptes personnels, l'un pour le majeur protégé et l'autre pour le mandataire judiciaire, adaptés à chaque mandat.

Les personnes détenues

Au nombre de 70.164 au 1er septembre 2018, les personnes détenues conservent une grande majorité de leurs droits qu'elles doivent pouvoir faire valoir : reconnaissance d'enfants, délivrance de papiers d'identité, constitution de dossiers de retraite, demande d'aide juridictionnelle, etc. Elles conservent également des obligations envers le service public, telle que la déclaration d'impôts.

En pratique, les conseillers pénitentiaires d'insertion et de probation doivent réaliser toutes ces démarches, notamment pour les détenus isolés socialement. Cependant, leur charge de travail ne permet pas de réaliser l'ensemble des démarches administratives pour l'ensemble des détenus. Les difficultés sont accentuées dans les maisons d'arrêt pour les détenus condamnés à des peines de très courte durée, ce qui ne permet pas l'aboutissement des démarches et donc les droits ouverts peuvent s'éteindre.

Le Défenseur des droits constate qu'en l'absence de connexion internet, les détenus sont dans l'impossibilité d'accéder à leurs droits. Un tel état de fait est contraire à l'article 130-1 du Code pénal qui assigne comme une des fonctions à la sanction pénale de favoriser l'insertion ou la réinsertion du détenu.

La dématérialisation des démarches administratives est pourtant une occasion à saisir pour faciliter l'accès aux droits des détenus en leur permettant d'effectuer à distance des démarches administratives.

Le Défenseur des droits recommande en conséquence de prendre en compte les publics spécifiques : permettre aux personnes détenues de disposer d'un accès effectif aux sites des services publics, des organismes sociaux ainsi qu'aux sites de formation en ligne agréés par l'Education nationale, généraliser le double accès aux comptes personnels pour le majeur protégé et son mandataire judiciaire.

Pour information

Avis du Défenseur des droits 18-04 du 14 février 2018 relatif au projet de loi n°259 pour un Etat de au service d'une société de confiance

Communiqué de presse du 20 septembre 2018 du Défenseur des droits appelant le Gouvernement à respecter les droits des usagers dans la dématérialisation des formalités administratives

Exemples de saisines traitées par le Défenseur des droits

Les conséquences des zones blanches dans l'accès aux droits

Monsieur X a été radié de Pôle emploi en raison de deux absences à des rendez-vous avec son conseiller. Or, Monsieur X. réside dans un secteur qualifié de « zone blanche » et n'a jamais reçu à temps les mails de convocation et les sms sur son téléphone portable. À la suite de l'intervention du Défenseur des droits, Pôle emploi est revenu sur sa décision de radiation.

L'absence de connexion internet et d'équipement informatique à domicile

Un couple de personnes résidant en Guadeloupe a constaté que le virement de l'Allocation aux Adultes Handicapés (AAH), dont ils étaient bénéficiaires, ne parvenait plus sur leur compte en banque. Ils se sont déplacés à la CAF et ont été informés qu'une notification de suspension de l'AAH leur avait été envoyée par courriel via leur compte CAF, mais que les délais pour déposer un recours amiable étaient dépassés. Or, âgés de 75 et 86 ans, ils ne disposaient ni d'un ordinateur, ni d'une connexion internet. L'abonnement internet coutant 40 euros par mois, ils indiquent ne pas en avoir les moyens financiers.

Après l'intervention du Défenseur des droits, la CAF a accepté leurs recours contre la décision.

La confusion entre site du service public et site de prestataires privés

Madame X achète fin janvier 2018 un véhicule d'occasion. Une fois tous les documents en sa possession elle tape sur un moteur de recherche internet, le mot « carte grise » pour réaliser sa démarche. Un site s'affiche en tête de liste qui, pour elle, est le site officiel : il y a un drapeau bleu blanc rouge et il est inscrit que le site est « habilité par le ministère de l'intérieur et agrémenté par le Trésor Public ».

Elle remplit le formulaire demandé, et joint le règlement de 204,76 euros pour finaliser sa demande le 24 février 2018. En juin 2018 on lui signale une erreur sur un document, il faut débourser 20 euros pour le rectifier. Le 12 juillet 2018, elle a de nouveau un retour lui indiquant que son dossier est en attente car le contrôle technique, obligatoirement de moins de 6 mois pour cette procédure, est expiré.

Madame X saisi le Défenseur des droits qui vérifie que son dossier est enregistré sur le site de l'ANTS, mais que la réclamante ne peut accéder à son dossier car il lui il faut le titre interbancaire de paiement (TIP) et le professionnel ne le lui a pas transmis. Le Défenseur des droits constate que l'usagère, de bonne foi, se retrouve dans l'impossibilité d'utiliser son véhicule et est contrainte de payer une nouvelle fois son contrôle technique alors qu'elle aurait pu réaliser sa démarche de manière autonome si elle n'avait pas été induite en erreur.

Des sites internet inadaptés

Monsieur X. ayant le statut de réfugié en France souhaite demander le revenu de solidarité active sur le site internet de la CAF. Lors de la demande en ligne, il doit indiquer s'il est étranger ou français et dans le premier cas la CAF lui demande s'il remplit la condition de résidence depuis plus de 5 ans. Etant réfugié depuis moins d'un an, il répond non. Le formulaire en ligne lui indique par conséquent qu'il n'est pas éligible au RSA car il ne remplit pas la condition d'antériorité de séjour. Or, la loi édicte que les personnes ayant le statut de réfugié, bien que de nationalité étrangère, ne sont pas soumises à cette condition d'antériorité.

M. X saisit le Défenseur des droits qui informe la CNAF de l'impossibilité de réaliser cette démarche en ligne pour les personnes réfugiées. Le 3 aout 2018, la CNAF a ajouté un libellé sur la case « condition de résidence depuis plus de 5 ans » indiquant que « si vous êtes réfugié, cocher oui à cette « question ».

L'absence de compte bancaire et le paiement dématérialisé

Le Défenseur des droits a été saisi d'une réclamation relative à la suspension du versement de la pension de retraite d'un assuré ne disposant pas de compte bancaire, à la suite de la décision de la CIPAV de verser les prestations exclusivement par virement bancaire et de cesser les paiements par chèque. Le Défenseur des droits a recommandé à l'organisme de procéder au paiement de la pension de retraite de Monsieur X. par un autre moyen que le virement bancaire et d'étendre la solution retenue à l'ensemble des assurés qui avaient été privés du paiement de leurs prestations pour la même raison.

Les conséquences d'un changement d'adresse mail lors d'une démarche administrative dématérialisée

Monsieur X., retraité, a changé de fournisseur d'accès à internet (FAI) et donc d'adresse de messagerie électronique. Il dispose depuis lors d'une nouvelle adresse de messagerie, son ancienne adresse n'existant plus. Il s'est retrouvé dans l'incapacité matérielle de se connecter à son compte fiscal via impots.gouv.fr car l'adresse électronique renseignée lors de la création de son espace personnel a été détruite par son FAI. Il lui est donc impossible de se connecter sur son compte fiscal pour signaler le changement d'adresse électronique et indiquer sa nouvelle adresse de messagerie électronique, afin de faire sa déclaration de revenus en ligne.

N'obtenant pas de réponse de la part de son service des impôts, il a sollicité le Défenseur des droits qui s'est rapproché des services informatiques de la direction générale des finances publiques (DGFIP) puis du service des impôts des particuliers, gestionnaire du dossier, qui a pu valider sa nouvelle adresse électronique sur son compte fiscal.

La non prise en compte des mandataires dans les démarches administratives en ligne des majeurs protégés

Malgré plusieurs tentatives, une mandataire judiciaire n'a pas pu créer de compte en ligne au nom de la majeure protégée pour laquelle elle assure une mesure de protection, puisque sur le site il est indiqué que les mandataires ne sont pas autorisés à s'inscrire et à accéder à l'espace personnel sécurisé de leur mandant. Un message invite donc les mandataires à contacter la caisse de retraite concernée par voie postale ou par téléphone afin de fixer un rendez-vous personnalisé. Néanmoins, ces autres canaux d'accès aux services publics sont très peu accessibles.

Suite à l'intervention du Défenseur des droits, la Caisse Nationale d'Assurance vieillesse a indiqué travailler sur le sujet et développer son offre de service en ligne et poursuivre cet investissement, notamment pour renforcer l'accès aux droits.

Editorial

Bruno Le Maire,
ministre de l'Économie, des Finances et de la Relance.

Amélie de Montchalin,
ministre de la Transformation et de la Fonction publiques

Cédric O,
secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques

La crise sanitaire actuelle a mis en évidence le caractère essentiel des outils numériques pour la résilience de notre société. Les organisations publiques comme privées ont accéléré fortement leur numérisation pour maintenir leur activité et proposer de nouveaux services. La plupart de ces services existent aujourd'hui grâce aux technologies d'informatique en nuage qui permettent d'héberger et de traiter les données des entreprises, des administrations et des citoyens.

Le Cloud représente trois enjeux majeurs pour la France : la transformation de nos entreprises et de nos administrations, la souveraineté numérique et la compétitivité économique.

Au fur et à mesure de la numérisation de nos sociétés, le Cloud a investi tous les pans de notre économie. Hier, seuls les géants du numériques y avaient recours ; demain dans tous les domaines de l'industrie et dans le secteur public, nous aurons recours au Cloud pour héberger et traiter toujours plus de données. Sans Cloud, pas de voiture autonome, pas d'éducation à distance, pas de chaines de production automatisées, pas de robots dans les blocs opératoires, pas de réseau électrique adapté aux énergies renouvelables, etc.

Dans les années à venir, le Cloud sera donc l'une des briques essentielles des innovations dans de nombreux secteurs. Une part croissante de nos services numériques s'appuie désormais sur le Cloud. Or ce marché du Cloud est dominé par des acteurs internationaux dont certains sont soumis à des lois à portée extraterritoriale qui pourraient exposer les données des citoyens, des administrations et des entreprises françaises à un risque de transfert hors de l'Union européenne.

Compte tenu de ce triple enjeu, transformation, compétitivité et souveraineté, le Gouvernement a décidé la mise en œuvre d'une stratégie nationale portant sur les technologies Cloud, en cohérence avec les initiatives européennes en la matière. Cette stratégie s'articule autour de 3 piliers que sont le label Cloud de confiance, la politique « Cloud au centre » des administrations et enfin une politique industrielle mise en œuvre dans le prolongement de France Relance. Notre but est clair : protéger toujours mieux les données des entreprises, des administrations et des citoyens français tout en affirmant notre souveraineté.

Introduction

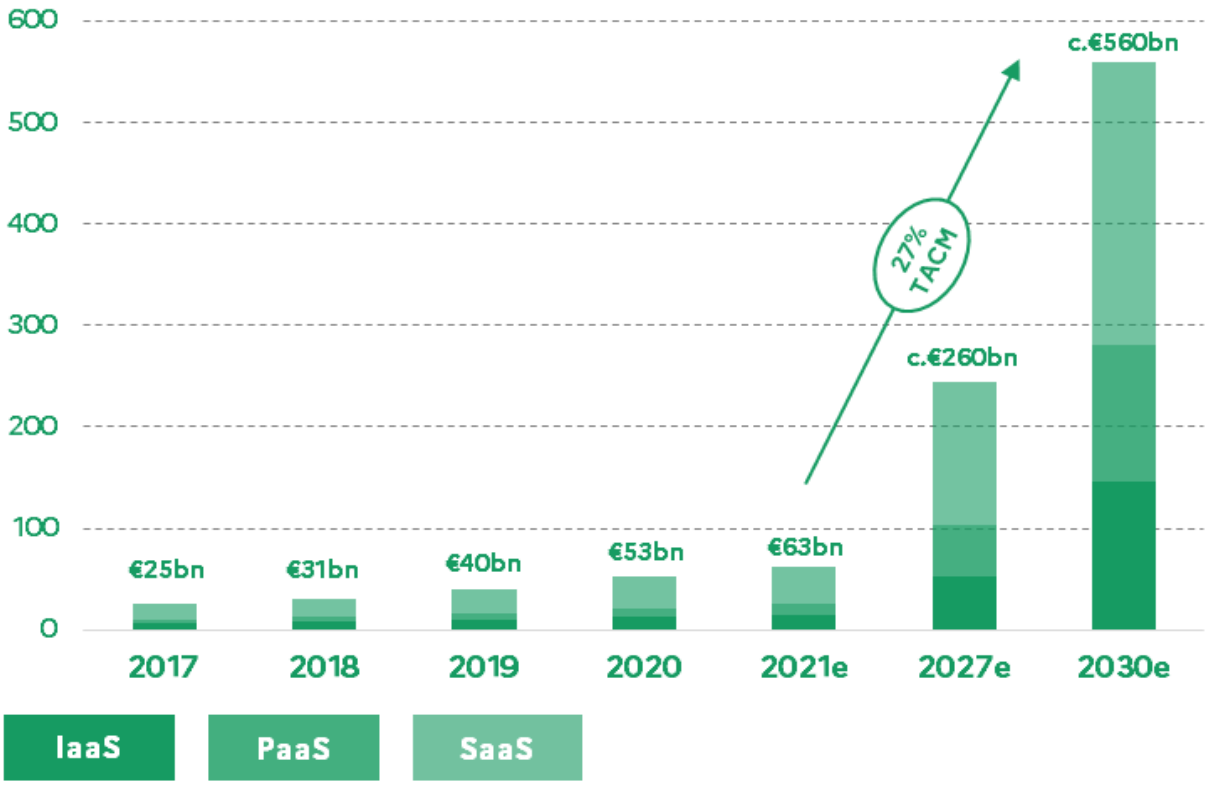
La crise sanitaire actuelle a mis en évidence toute l'importance des services numériques. La plupart de ces services existent aujourd'hui grâces aux technologies d'informatique en nuage qui permettent d'héberger et de traiter les données des entreprises, des administrations et des citoyens via un accès réseau. **Envoyer un e-mail, partager une photographie ou reserver un rendez-vous médical ne peut ainsi plus se faire sans recourir au Cloud.** Les entreprises et les administrations peuvent également recourir à une large palette de services technologiques permis par le Cloud.

Toutes ces solutions offrent au client une grande flexibilité, une optimisation des coûts et surtout l'accès à des solutions performantes, innovantes et sécurisées. Avec la numérisation de notre société, la place et l'importance du Cloud ont grandi. Demain dans tous les domaines de l'industrie, dans le secteur public, dans l'éducation ou encore dans la santé, l'usage du Cloud sera nécessaire à la croissance de notre économie[1].

« Le cloud est désormais le socle incontournable pour nos entreprises et administrations publiques. La souveraineté numérique de l'Europe est intimement liée à sa capacité à maîtriser ses dépendances sur le marché du cloud, notamment en développant des services de cloud de confiance et en généralisant l'usage. »

Bernard Duverneuil, Président du Cigref
Group Chief Digital & Information Officer, Elior Group

Taille du marché du Cloud en Europe[1]



[1] Source : Etude KPMG Avril 2021

Le recours à des solutions cloud n'en est qu'à ses débuts. Dans les années à venir, le Cloud sera l'une des briques essentielles des innovations dans de nombreux secteurs. La croissance annuelle du secteur est ainsi supérieure à 20%, multipliant la taille du marché européen par 10 en dix ans. Le cloud pourrait ainsi atteindre la taille du secteur des télécommunications d'ici 2030 et créer de nombreux emplois en Europe. Le plein essor du secteur du cloud est une opportunité économique unique pour l'Europe et pour la France.

Néanmoins, le marché est actuellement dominé par des acteurs étrangers qui peuvent imposer des conditions de sorties très complexes : les entreprises se retrouvent souvent dépendantes de leur fournisseur cloud. Cette domination complexifie l'émergence d'acteurs européens et pose également un fort risque de captation des données, certains pays ayant adoptés des législations à portée extraterritoriale leur permettant d'accéder aux données stockées. Cette situation met à mal la souveraineté européenne. L'Europe doit veiller à garder la main sur la pleine gestion de ses données personnelles et industrielles.

« Le cloud s'est imposé comme un outil essentiel d'innovation et de performance pour les grandes entreprises françaises comme Engie. Il est indispensable d'en renforcer la maîtrise sous tous ses aspects. »

Yves Le Gélard, Group Chief Information & Digital Officer, Engie

Pour répondre à ces enjeux, le Gouvernement a élaboré une stratégie reposant sur 3 piliers : un nouveau label cloud de confiance qui permettra aux entreprises et administrations françaises de bénéficier des meilleurs services offerts par le Cloud (suites bureautiques collaboratives, outils de visioconférence, etc.) tout en assurant la meilleure protection pour leurs données ; la politique « Cloud au centre » de l'administration pour accélérer résolument la transformation numérique du service public ; une stratégie industrielle ambitieuse, inscrite dans le cadre de France Relance, qui permettra d'assoir la souveraineté française et européenne accompagnant la construction de nouveaux outils *Cloud.*

Stratégie Nationale pour le *Cloud*

I. LABEL CLOUD DE CONFIANCE	Un nouveau label pour bénéficier des meilleurs services *Cloud* mondiaux tout en protégeant les données des français
II. CLOUD AU CENTRE	Moderniser l'action publique grâce aux technologies du *Cloud*
III. POLITIQUE INDUSTRIELLE	France Relance au service de la souveraineté française pour accompagner la construction de nouveaux services *Cloud*

I. Un nouveau label : le Cloud de confiance

Le **niveau de protection le plus élevé pour les données des Français** est la priorité de la politique de *Cloud* du Gouvernement. Cette sécurisation doit opérer aux niveaux technique comme juridique. En effet, si les caractéristiques techniques permettent de lutter contre les risques de cybermalevillance, le niveau juridique doit conduire à se prémunir des risques d'application de lois extraterritoriales non conformes aux valeurs européennes. C'est à cette double problématique que répond le *Cloud* de confiance dans un but clair : protéger les données des entreprises, des administrations et des citoyens français.

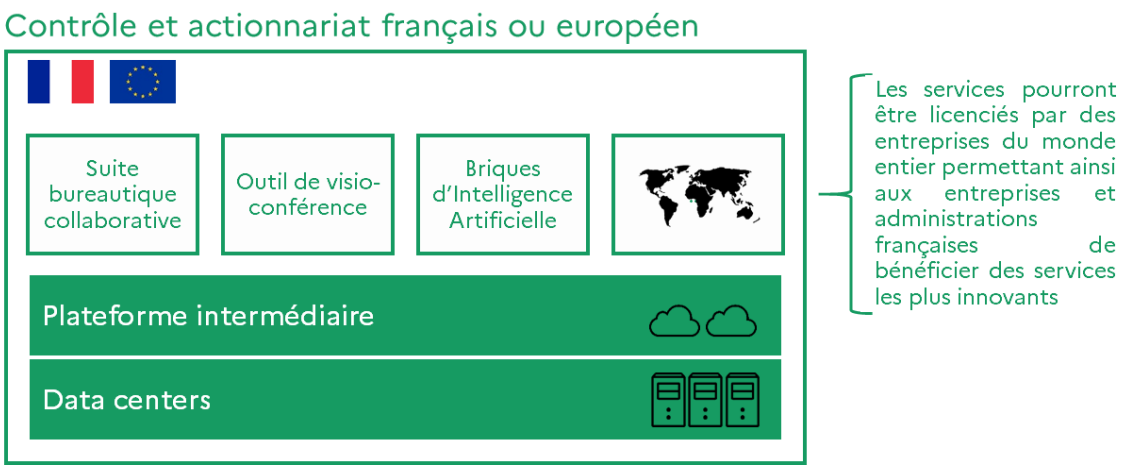
« Le cloud n'est plus une option, mais une nécessité que ce soit en termes économiques, de délai de mise à disposition de solutions innovantes ou encore de mitigation des risques. Une doctrine commune clarifiant les caractéristiques d'un label pour le "cloud de confiance" est un facteur clé de succès dans l'adoption de ces services et la bonne mise en œuvre de nos projets de transformation numérique. »

Gilles Lévêque, Directeur des Systèmes d'Information, groupe ADP

Ce label *Cloud* de confiance offrira donc un double niveau de sécurisation – juridique et technique – et **permettra aux entreprises et administrations françaises de bénéficier des meilleurs services Cloud**. Certains des services Cloud les plus performants au monde sont édités par des entreprises extra-européennes : ces services pourront également être labellisés sous certaines conditions portant notamment sur l'entité opérant ces services et sur la localisation des données. Le label Cloud de confiance permettra ainsi de nouvelles combinaisons comme la création d'entreprises alliant actionnariat européen et technologies étrangères sous licence. Cette politique répond à un besoin clair : **donner accès au meilleur niveau de service tout en respectant les valeurs européennes**.

Ce nouveau label intervient enfin comme une **réponse aux attentes des petites et grandes entreprises françaises** en traçant une voie claire pour les Organismes d'Intérêts Vitaux (OIV) mais également pour le reste des acteurs économiques et administrations pour qui la sécurisation des données des Français est une priorité.

Schéma d'offres hybrides compatibles Cloud de confiance



« Les données sont la richesse du futur. L'Europe doit s'organiser pour préserver ce patrimoine, tout en favorisant en son sein les échanges. Disposer d'un Cloud de confiance est le prérequis, la fondation, qui nous permettra collectivement de tirer parti de cette ressource clé et bâtir sur cette base les usages et services de demain pour nos clients. »

Christophe Leblanc, Directeur des ressources et de la transformation numérique, Société Générale

Afin d'assurer, par construction, une protection aux risques d'accès aux données du fait de l'application de réglementations extraterritoriales et d'obtenir le Visa de sécurité SecNumCloud, les solutions devront respecter les conditions suivantes :

- Remplir les exigences de sécurité associées au référentiel technique SecNumCloud[2] ;
- Localiser les infrastructures et opérer les systèmes en Europe ;
- Assurer les portages opérationnel et commercial de l'offre par une entité européenne, détenue par des acteurs européens.

Le Gouvernement engage donc une démarche de promotion du Visa de sécurité SecNumCloud au travers du label Cloud de confiance auprès des grandes entreprises, des entreprises stratégiques, ainsi que des administrations. Il portera également les exigences de ce Visa de sécurité lors de la définition du niveau élevé du futur schéma européen (*European Cybersecurity Certification Scheme for Cloud Services*).

« Air France KLM accueille avec un grand intérêt cette stratégie d'accélération en faveur du cloud de confiance, lequel constitue un atout pour l'hébergement de certaines applications et données hautement critiques nécessitant un niveau de protection et de garanties supplémentaires, tout en bénéficiant des meilleures avancées technologiques. »

Jean-Christophe Lalanne, Directeur des Systèmes d'Information, Air France-KLM

Enfin, en complément du Visa de sécurité SecNumCloud, le Gouvernement encourage les fournisseurs de solutions Cloud à mettre en œuvre **des garanties en termes de réversibilité, d'interopérabilité, de portabilité, et de transparence au travers notamment de l'initiative Gaïa-X.**

« Dans un monde de plus en plus numérique, EDF doit pouvoir s'appuyer sur des environnements de confiance, souverains et sécurisés, notamment pour développer ses projets industriels avec ses partenaires ou construire de nouveaux services qui accompagnent la transition énergétique.
C'est pourquoi EDF est engagé au niveau français en pilotant le Groupe de Travail Cloud de confiance du CIGREF et au niveau européen en tant que membre fondateur de Gaia-X, membre du board des directeurs et pilote du dataspace Energy.
La stratégie Cloud de l'Etat, le label qu'elle introduit et les engagements qu'elle porte répondent pleinement à nos enjeux. »

Véronique Lacour, Directeur exécutif Groupe en charge de la Transformation et de l'Efficacité Opérationnelle, EDF

[2] https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf

II. Transformation numérique de l'Etat : une nouvelle politique Cloud au centre

Avec l'adoption de la doctrine « Cloud au centre », le Gouvernement fait du Cloud un prérequis pour tout nouveau projet numérique au sein de l'État, afin d'accélérer la transformation publique au bénéfice des usagers et dans le strict respect de la cybersécurité et de la protection des données des citoyens et des entreprises.

L'État doit mobiliser les meilleures pratiques et innovations numériques pour répondre aux enjeux d'amélioration du service public. La doctrine d'utilisation de l'informatique en nuage par l'Etat de novembre 2018 faisait du Cloud un levier prioritaire de la transformation numérique de l'État. L'expérience acquise durant les deux dernières années permet à présent au Gouvernement d'accélérer la transition vers le Cloud des administrations en adoptant une approche « Cloud au centre ».

Accélérer la transformation numérique de l'État

Le Cloud est essentiel pour **accompagner et accélérer l'évolution des pratiques** de développement de produits numériques de l'État. La nouvelle doctrine cordonnée par le ministère de la transformation et de la fonction publiques permet d'inscrire ce virage durablement dans les directions du numérique des ministères et plus largement auprès de tous les acteurs de l'État.

L'adoption du Cloud doit permettre de **faciliter la mise en œuvre des engagements du Gouvernement en matière de transformation numérique des administrations**. Le Cloud doit conduire à équiper les agents de meilleurs outils de travail numériques, plus collaboratifs, et d'améliorer durablement les démarches des usagers en ligne, qu'ils soient citoyens ou entreprises.

Des exemples de projets numériques de l'Etat hébergés dans le cloud

- Tchap, la messagerie instantanée sécurisée des agents publics, est hébergée sur le cloud du ministère de l'Intérieur.
- Histovec, qui garantit plus de confiance lors de la vente d'un véhicule d'occasion grâce à la possibilité pour l'acheteur d'accéder à l'historique des faits marquants du véhicule, a été développé en quelques mois grâce au cloud.
- Osmose, la plateforme collaborative de l'État et de ses établissements publics est hébergée sur un cloud commercial et compte aujourd'hui plus de 50 000 utilisateurs. Elle est l'une des outils du sac à dos numérique de l'agent public (SNAP) favorisant le travail en mobilité.

Enfin, ce virage doit permettre de répondre aux attentes légitimes des Français d'exemplarité de l'Etat en matière de **protection de leurs données** ainsi qu'en termes de garantie de la **continuité du service public**, deux prérequis à leur confiance dans le service public numérique.

La nouvelle doctrine « Cloud au centre »

Cette nouvelle doctrine s'applique aux **ministères et organismes placés sous leur tutelle,** et s'incarnera dans une circulaire. Le Cloud devient **dorénavant la méthode d'hébergement par défaut pour les services numériques de l'Etat,** pour tout nouveau produit numérique et pour les produits connaissant une évolution substantielle. Les recrutements et les programmes de formation continue destinés aux agents publics dans la filière numérique comporteront un volet Cloud.

« Le cloud est une formidable opportunité pour accélérer la transformation numériques des administrations. Utiliser les meilleures solutions numériques disponibles est essentiel pour améliorer la qualité des services publics en ligne ainsi que doter les agents publics d'outils numériques plus modernes et plus collaboratifs. La doctrine "cloud au centre" va contribuer à un service public de meilleure qualité tout en garantissant la sécurité et la protection des données des citoyens et une souveraineté numérique renforcée. »

Nadi Bou-Hanna, directeur interministériel du numérique

Les services numériques des administrations seront hébergés sur **l'un des deux cloud interministériels internes de l'Etat ou sur les offres de Cloud proposées par les industriels satisfaisant des critères stricts de sécurité.**

Notamment, chaque produit numérique manipulant des **données sensibles**, qu'elles relèvent notamment des données personnelles des citoyens français, des données économiques relatives aux entreprises françaises, ou d'applications métiers relatives aux agents publics de l'Etat, devra impérativement être hébergé sur le cloud interne de l'Etat ou **sur un cloud industriel qualifié SecNumCloud par l'ANSSI et protégé contre toute réglementation extracommunautaire**.

Le passage au cloud est enfin une occasion de **renforcer la résilience des produits numériques des administrations**, au service de la continuité du service public. Les administrations s'appuieront donc sur une diversité de technologies, de fournisseurs et d'infrastructures et préparerons des **plans de continuité et de reprise d'activité** pouvant être activés en cas d'incident.

« Le numérique a permis une fantastique démocratisation de l'information géographique. Il faut maintenant créer des alliances entre l'Etat, les collectivités territoriales et des comunautés ouvertes pour mettre les géodonnées en partage face à la domination des géants du numérique et aux enjeux climatiques. Pour cela, le cloud est une brique incourtournable pour passer à l'échelle. »

Sébastien Soriano, directeur général de l'IGN

Avec « Cloud au centre », le Gouvernement se dote d'une doctrine complète, engageant résolument les administrations sur la voie d'une transformation numérique de qualité tout en renforçant la souveraineté de l'Etat et la protection des données des Français.

III. France Relance et le PIA IV au service de la souveraineté technologique française

Le troisième pilier de la stratégie Cloud de l'Etat consiste en un soutien direct à des projets à forte valeur ajoutée dans le cadre du 4ème Programme d'Investissements d'Avenir et de France Relance. Cette action identifiera et soutiendra des projets industriels de développement de technologies. Elle vise notamment les technologies critiques telles que les solutions PaaS pour le déploiement de l'intelligence artificielle et du big data ou encore les suites logicielles de travail collaboratif.

Un Appel à manifestation d'intérêt : « Développement et renforcement de la filière française et européenne du Cloud » | Bpifrance servir l'avenir est ainsi ouvert jusqu'au 17 mai 2021.

« Pour soutenir ses objectifs de neutralité carbone, Total accélère sa transformation numérique. Le Groupe a l'ambition d'utiliser toute la capacité des outils digitaux pour innover dans l'ensemble de ses métiers et veut tirer parti de la puissance des solutions cloud pour y parvenir.Dans un contexte marqué par l'émergence de la cybercriminalité et la montée des réglementations extraterritoriales, Total accueille la publication de la stratégie cloud de confiance de l'Etat avec grand intérêt. En effet, elle favorisera l'émergence d'offres de service qui répondront à ses besoins de protection technique et juridique de ses données et permettront de tirer parti en confiance de la révolution numérique au service de la transition énergétique. »

Patrick Pouyanné, Président-directeur général de Total

Lors des premières relèves intermédiaires, 5 projets ont été déposés, pour une assiette totale de 107 M€. Ils impliquent des grands groupes, des PME, des start-ups et des organismes de recherche, et couvrent les domaines des plateformes de travail collaboratives, du *edge-computing*, notamment dans le contexte de l'IoT, ainsi que des communications sécurisées. Pour les projets présélectionnés, les auditions interviendront environ un mois après les relèves.

Ces projets pourront par exemple soutenir le développement de plateformes de Edge Computing permettant aux industriels de gérer en temps réel les milliers d'équipements et capteurs présents par exemple dans les usines ou sur les réseaux de distribution d'eau et d'électricité. De telles plateformes sont nécessaires notamment pour automatiser des chaînes de production et créer des jumeaux numériques de ces réseaux, éléments essentiels à la ré-industrialisation française.

Les premiers projets débuteront dans les prochains mois tandis que les plus importants d'entre eux seront financés dans le cadre d'un Projet Important d'Intérêt Européen Commun (PIEEC) réunissant à ce jour 11 Etats membres : la France, l'Allemagne, l'Italie, l'Espagne, la Belgique, le Luxembourg, la Slovénie, la Hongrie, la Tchéquie, la Pologne et la Lettonie. Ce PIEEC aura notamment pour ambition de développer une offre de *Cloud* européenne verte dans les domaines de rupture technologique, tels que le *edge computing*. Typiquement, **ce PIEEC permettra la mobilisation de fédérations d'acteurs dans l'optique de créer des projets transformant tels qu'une suite de bureautique collaborative européenne.**

« Enedis, en tant qu'opérateur de confiance, accorde une importance majeure à l'hébergement des données énergétiques de ses clients et des territoires ;

l'émergence d'un cloud de confiance répond à notre souhait de pouvoir utiliser sereinement les solutions du marché tout en protégeant nos informations sensibles »

Jean-Claude Laroche, Directeur des systèmes d'information, Enedis

La capacité à traiter des données au plus proche de l'endroit où elles sont recueillies est critique pour certaines applications (voiture autonome par exemple) qui ne peuvent tolérer des temps de latence, des pannes réseaux, etc. L'un des enjeux de cette nouvelle approche dite de *edge computing* est son intégration avec le *Cloud* ainsi que l'orchestration des futurs réseaux dans un continuum *Edge-Cloud*.

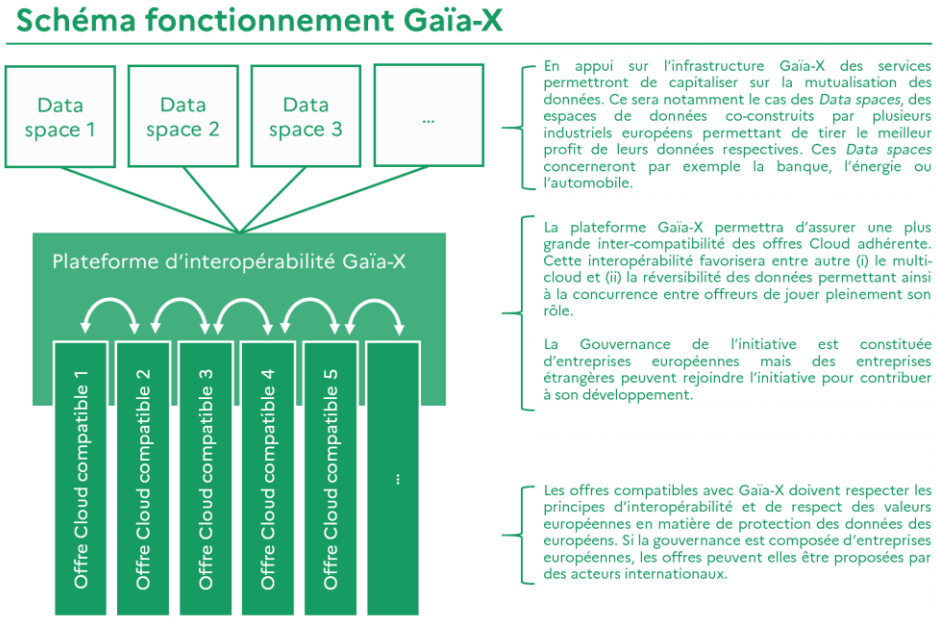
« Le besoin d'un cloud de confiance disposant d'un large catalogue de services a été clairement exprimé par les membres du Cigref, afin de garantir la sécurité de leurs données sensibles et des traitements associés, clarifier le régime juridique auquel elles sont soumises et les préserver des législations extra-européennes, et maîtriser leurs dépendances vis-à-vis de leurs fournisseurs. »

Vincent Niebel, Pilote du groupe de travail « cloud de confiance » du Cigref, Directeur des systèmes d'information, EDF

Pourquoi GAIA-X ?

La fluidité du marché du *Cloud* ne doit pas être entravée par des difficultés techniques liées au changement de fournisseur, ou à l'intégration verticale des solutions.

A ce titre, le Gouvernement soutient pleinement l'association GAIA-X et l'architecture de standards qu'elle mettra en œuvre. Ainsi, les entreprises européennes pourront, grâce à GAIA-X, comparer, sélectionner et construire des solutions *Cloud* avec l'assurance que leurs données resteront sous leur contrôle en permettant de changer de fournisseur de *Cloud* de manière simplifiée.



Ce soutien se traduira également par le financement des services de fédération de la plateforme GAIA-X et de la création d'espaces de données partagées au sein de la filière industrielle. Ces espaces de données regroupant les données d'acteurs industriels d'une même filière permettront l'émergence de nouveaux usages et la valorisation de données trop souvent disséminées entre de nombreux acteurs. **Un appel à projets pour la mutualisation des données est d'ores et déjà ouvert pour l'année 2021 et sera prolongé au-delà de 2022. Ce dispositif a d'ores et déjà permis de financer 11 projets depuis 2018, pour une aide publique de 40 M€.**

Appel à projets ATF : Plateformes numériques et mutualisation de données pour les filières | Bpifrance servir l'avenir

« En tant qu'acteur institutionnel français très engagé depuis les débuts du projet Gaia-X aux côtés des autres acteurs de la place, la Caisse des Dépôts considère l'émergence de solutions de cloud de confiance comme un facteur déterminant visant à construire un écosystème européen de données de confiance. En tant qu'acteur financier majeur et souverain, nous soutenons l'initiative prise par l'Etat dans le cadre de sa stratégie cloud »

Olivier Sichel, Directeur Général Délégué de la Caisse des Dépôts

Enfin, parce que la recherche et la formation sont le moteur de l'innovation, un Programme et Equipements Prioritaires de Recherche est à l'étude afin de garantir que la France soit à la pointe des technologies en matière de *Cloud*, en complément d'un renforcement de l'offre de formations initiale et continue.

Qu'est-ce qu'un PIEEC (ou IPCEI en anglais) ?

- Ensemble de projets formant un projet dit « intégré » de très grande envergure qui implique une collaboration renforcée des partenaires sélectionnés par les Etats membres et destiné à répondre à une problématique commune définie par ces derniers.
-
- Objectifs : (i) accroître la R&D&I et créer des retombées significatives sur le marché unique ; (ii) permettre les premiers déploiements industriels impliquant la mise au point d'un nouveau produit ou service ou d'un nouveau processus innovant ; (iii) accroître la protection de l'environnement, favoriser l'efficacité énergétique ou favoriser la mobilité durable.
- Les retombées du projet doivent être significatives pour l'ensemble de l'Union.
- Les projets doivent être cofinancés par les porteurs.
- Le projet intégré doit être validé par la Commission Européenne ainsi que chaque projet qui en fait partie.

Objectifs du PIEEC *Cloud* - Souveraineté numérique européenne et développement économique : l'Europe doit se doter des infrastructures et des services qui permettront de valoriser les données produites notamment par les industriels ainsi que le développement de l'IoT.

DOCUMENT 7
« Bleu: renouveau ou mirage du cloud souverain 2.0 » - lemondeinformatique.fr - 31 mai 2021

L'annonce surprise conjointe de Capgemini et Orange de créer la co-entreprise Bleu pour servir de tête de point aux services cloud de Microsoft répondant aux enjeux de souveraineté des données pose question. Les ambitions sont pourtant réelles.

Loin d'être attendue, l'annonce de Capgemini et Orange pour fonder (à parité) une société cloud commune - Bleu - a eu de quoi surprendre. D'autant plus que pour répondre aux enjeux et problématiques des entreprises et également des grands clients OIV et OSE français, ce sont des solutions Microsoft (Azure et Office 365) qui sont à ce jour exclusivement proposées. Un choix intriguant quant on sait que les solutions étrangères notamment américaines comme Microsoft (mais aussi AWS, Google...) sont soumises à des réglementations comme le Cloud Act. Avec à la clé une possible extra-territorialité des données. Un paramètre parfaitement assumé par les principaux intéressés et en particulier Orange.

« On va avoir sans aucun doute possible une totale étanchéité par rapport à l'extra-territorialité des données », nous a assuré Cédric Parent, directeur général adjoint des activités cloud d'Orange. « Il n'y aura aucune manipulation de données, patching et opérations en dehors d'un personnel qui ne serait pas de la société Bleu ». Cette société, co-créée par Orange et Capgemini - rejoint par un autre actionnaire de référence dont l'identité n'est à ce jour pas publique - sera de droit français et constituée dans le courant de cet été. Plusieurs datacenters répartis en France - sans doute localisés chez Interxion ou Equinix - sont prévus pour fournir un éventail très large de services cloud Azure et Office 365 mais également devops.

Bleu plus fort qu'un partenariat ou une alliance

A ce stade, la répartition exacte des ressources entre celles proposées par Orange et Capgemini n'a pas été précisée. Tout comme la gouvernance et l'équipe de direction. Dans les équipes opérationnelles, il s'agira principalement de recrutements pour l'occasion et non d'un rapatriement de ressources humaines provenant d'Orange et Capgemini vers Bleu. « Il s'agit d'une combinaison du meilleur des deux mondes entre confiance et souveraineté ainsi que richesse et fonctionnalités », nous a expliqué Helmut Reisinger, directeur général d'OBS. « Il s'agit d'une offre jamais vue sur les marchés avec l'accès aux meilleurs équipes et outils de travail les plus efficaces ».

Interrogés sur la pertinence de Bleu par rapport à d'autres offres de cloud poussées en France - on pense à l'accord entre Atos et OVHcloud (avec qui OBS est par ailleurs aussi partenaire) - les dirigeants d'Orange considèrent Bleu comme autre chose qu'un « simple » partenariat ou alliance. « Il s'agit de quelque chose de différent où il y aura de nouveaux services IaaS, mais aussi SaaS et toute une partie PaaS qui permet de gérer les big data et l'IA, mais aussi des ressources GPU pour apporter de la puissance aux plateformes de développement », poursuit Cédric Parent.

Un design platform approuvé par l'ANSSI

Dans le cadre de Bleu, Orange assure avoir travaillé « main dans la main » avec l'Anssi et le gouvernement pour leur présenter le design de leur plateforme qui a apparemment été validé. « On a eu les premiers retours et on respecte les processus pour entrer dans les critères SecNumCloud et cloud de confiance », poursuit Cédric Parent. Pour l'instant, on attend toujours une mise à jour officielle du référentiel SecNumCloud prenant compte de la certification en cours de Bleu en la matière. Par ailleurs, il est aussi prévu que Bleu rejoigne Gaia-X, ce qui parait assez logique et pourrait permettre dans le même temps à Microsoft de bénéficier par cet intermédiaire des labels SecNumCloud et Gaia-X. Autant dire de précieux sésames pour espérer - par exemple ? - revenir sur le devant de la scène après la polémique autour du Health Data Hub et des marche-arrière du ministère de la Santé et de l'Assurance Maladie qui pourraient alors décider de revoir leur décision.

Gorodenkoff/Adobestock

La stratégie présentée par le gouvernement le 17 mai 2021 ne résout pas totalement la question de la souveraineté des données.

Fini la souveraineté, place aux labels de confiance. On peut résumer ainsi la nouvelle stratégie « cloud » dépeinte par le gouvernement le 17 mai. Deux clouds hébergés par l'Etat seront mis en place, destinés aux ministères de l'Intérieur et de l'Economie. Pour les autres services, l'hébergement devra être fait sur un cloud « de confiance », labellisé par l'Anssi. Si la libre administration des collectivités territoriales ne les oblige en rien à changer leurs pratiques, le ministère de la Transformation et de la fonction publique les encourage à utiliser de manière volontaire les opportunités du cloud, en se dirigeant vers ces offres labellisées.

Simplicité du système

« Le système mis en place a l'avantage d'être simple à comprendre, estime Emmanuel Vivé, directeur général de l'Association pour le développement et l'innovation numérique des collectivités. La labellisation par l'Anssi est un gage de confiance et le système de licence, qui permet aux éditeurs d'héberger leurs solutions dans des clouds labellisés, montre une prise en considération de la réalité du terrain. Aujourd'hui, on déborde de demandes de formation sur Teams et les autres outils d'Office 365. »

Le système de licence présenté par l'Etat pouvait déjà s'observer en octobre, lorsque Google avait officialisé un partenariat avec OVH Cloud. Cet accord permet le déploiement et la vente par OVH de la plateforme Google Anthos : Google devient un éditeur de logiciels comme un autre, dont les services sont opérés par un prestataire européen, qui met à disposition un serveur labellisé par l'Etat. Les

services en ligne de Microsoft, également cités par Bruno Le Maire lors de la présentation de la doctrine du gouvernement, seront notamment disponibles dans Bleu, association entre Capgemini et Orange pour fournir un cloud « de confiance ».

Hébergement en Europe

Le choix du gouvernement est de proposer un hébergement en Europe, voire en France, plus protecteur juridiquement, avec cependant un accès aux services offerts par les grandes entreprises américaines. « Il faut être prudent, nuance Bertrand Serp, vice-président [LR] chargé du numérique à Toulouse métropole et membre du bureau de France Urbaine. Avec une licence, on devient propriétaire du service, mais comment être sûr que les données ne sont pas rapatriées ailleurs ? Et comment l'Etat peut-il garantir qu'une entreprise labellisée ne sera pas rachetée par des acteurs non européens ? Que l'Etat investisse davantage dans ces questions est une bonne chose, mais il ne faut pas toujours aller vers plus d'externalisation. Nos vies sont gérées par le numérique et l'Etat doit rester maître de ses choix. Il ne doit pas être caution, il doit être régulateur. »

France Urbaine, qui prépare un livre blanc sur le sujet, préfère, dans le doute, rediriger les collectivités vers des services locaux.

FOCUS

L'offre de l'Ugap s'adaptera rapidement

« Nous ne connaissons pas encore les délais de mise en place du label "cloud", mais notre questionnaire d'aide au choix évoluera en quelques jours une fois qu'il sera effectif », explique Sandra Chatillon, de l'Ugap. L'organisme propose déjà plusieurs offres de cloud destinées aux acteurs publics et le label sera un choix facultatif, comme Secnumcloud l'est déjà aujourd'hui.

« Les acteurs américains restent dans notre catalogue, notamment pour des utilisations avancées, par exemple lorsque des outils d'intelligence artificielle sont nécessaires », poursuit Sandra Chatillon. Selon l'Ugap, les « clouds de confiance » vont d'abord répondre aux besoins de stockage, avant de devenir un facteur discriminant pour des logiciels en ligne.

(...)

DOCUMENT 9

« Référentiel général de sécurité (extrait) - *Agence nationale de la sécurité des systèmes d'information* - 13 juin 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre	
Agence nationale de la sécurité des systèmes d'information (ANSSI)	**Secrétariat général pour la modernisation de l'action publique (SGMAP)**

RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ

version 2.0

HISTORIQUE DES VERSIONS		
DATE	**VERSION**	**ÉVOLUTION DU DOCUMENT**
06/05/2010	1.0	*Publication de la première version du Référentiel général de sécurité*
13/06/2014	2.0	*Publication de la deuxième version du Référentiel général de sécurité*

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information
SGDSN/ANSSI
Bureau de la maitrise des risques
et de la réglementation
51 boulevard de La Tour-Maubourg
75700 Paris 07 SP
rgs [at] ssi.gouv.fr

Le présent référentiel ainsi que les annexes sont disponibles en ligne sur les sites suivants :

- le site institutionnel de l'ANSSI (www.ssi.gouv.fr) ;
- le site institutionnel du SGMAP (www.references.modernisation.gouv.fr).

Le présent référentiel est pris en application du décret n° 2010-112 du 2 février 2010, lui-même pris pour l'application des articles 9, 10 et 12 de de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Il est publié par l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

Ce référentiel remplace la première version du référentiel général de sécurité publiée par arrêté du Premier ministre le 6 mai 2010. Il complète les règles et les recommandations relatives aux certificats électroniques et contremarques de temps et permet la qualification des prestataires d'audit de la sécurité des systèmes d'information. Les mécanismes de transition entre la première et la deuxième version du référentiel sont décrits dans le chapitre 8 du présent document.

Il fait l'objet de recommandations de mise en œuvre décrites sur la page http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/recommandations-relatives-a-la-mise-en-oeuvre-du-rgs.html.

Les termes entre « [ ] » renvoient aux références documentaires décrites dans le chapitre 10 du présent document.

Sommaire

Chapitre 1. Mise en conformité avec les exigences du « décret RGS »..... 5

Chapitre 2. Description des étapes de la mise en conformité 6

2.1 Analyse des risques 6
2.2 Définition des objectifs de sécurité 6
2.3 Choix et mise en œuvre des mesures de sécurité adaptées 6
2.4 Homologation de sécurité du système d'information 7
2.5 Suivi opérationnel de la sécurité du système d'information 7

Chapitre 3. Règles relatives à la cryptographie et à la protection des échanges électroniques..... 8

3.1 Règles relatives à la cryptographie 8
3.2 Règles relatives à la protection des échanges électroniques 8

Chapitre 4. Règles relatives aux accusés d'enregistrement et aux accusés de réception 12

Chapitre 5. Qualification des produits de sécurité et des prestataires de services de confiance . 13

5.1 Qualification des produits de sécurité 13
5.2 Qualification des prestataires de services de confiance (PSCO) 13

Chapitre 6. Validation des certificats par l'État..... 15

6.1 Champ d'application 15
6.2 Règles de sécurité 15
6.3 Procédure de validation 16
6.4 Liste des informations relatives à la délivrance et à la validation 16

Chapitre 7. Recommandations relatives à l'application du référentiel 17

7.1 Organiser la sécurité des systèmes d'information ____ 17
7.2 Impliquer les instances décisionnelles ____ 17
7.3 Adapter l'effort de protection des systèmes d'information aux enjeux de sécurité et prendre en compte la SSI dans les projets ____ 18
7.4 Adopter une démarche globale ____ 18
7.5 Informer et sensibiliser le personnel ____ 18
7.6 Prendre en compte la sécurité dans les contrats et les achats ____ 18
7.7 Prendre en compte la sécurité dans les projets d'externalisation et d'informatique en nuage ____ 19
7.8 Mettre en place des mécanismes de défense des systèmes d'information ____ 19
7.9 Utiliser les produits et prestataires labellisés pour leur sécurité ____ 20
7.10 Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité ____ 20
7.11 Procéder à des audits réguliers de la sécurité du système d'information ____ 20
7.12 Réaliser une veille sur les menaces et les vulnérabilités ____ 21
7.13 Favoriser l'interopérabilité ____ 21

Chapitre 8. Transition entre la première et la deuxième version du RGS 22

Chapitre 9. Liste des annexes du RGS 23

9.1 Documents applicables concernant l'utilisation de certificats électroniques ____ 23
9.2 Documents applicables concernant l'utilisation de mécanismes cryptographiques ____ 23
9.3 Référentiel d'exigences applicables aux prestataires d'audit de la SSI ____ 23

Chapitre 10. Références documentaires 24

10.1 Références réglementaires ____ 24
10.2 Références techniques ____ 24

Chapitre 1. Mise en conformité avec les exigences du « décret RGS »

Le référentiel général de sécurité (RGS) vise à renforcer la confiance des usagers dans les services électroniques proposés par les autorités administratives, notamment lorsque ceux-ci traitent des données personnelles. Il s'applique aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et avec les usagers. Il peut aussi être considéré comme un recueil de bonnes pratiques pour tous les autres organismes.

Afin de mettre leur système d'information en conformité avec le RGS, les autorités administratives doivent adopter une démarche en cinq étapes, prévue par le décret n° 2010-112 du 2 février 2010 (décret RGS) :

1. réalisation d'une analyse des risques (art. 3 al. 1) ;
2. définition des objectifs de sécurité (art. 3 al. 2) ;
3. choix et mise en œuvre des mesures appropriées de protection et de défense du SI (art. 3 al. 3) ;
4. homologation de sécurité du système d'information (art. 5) ;
5. suivi opérationnel de la sécurité du SI.

Dans l'éventualité où le système d'information serait déjà en service sans avoir fait l'objet de cette démarche, ou bien a été modifié, la procédure simplifiée suivante peut être mise en oeuvre :

1. réalisation d'un audit de la sécurité du système d'information en interne ou externalisé auprès d'un prestataire ;
2. réalisation d'une analyse des risques simplifiée ;
3. mise en œuvre des mesures correctives fixées dans le rapport d'audit ;
4. décision d'homologation de sécurité du système d'information ;
5. suivi opérationnel de la sécurité du SI.

Au-delà des mesures techniques et organisationnelles, les autorités administratives doivent veiller :

- aux clauses relatives à la sécurité des contrats qu'elles passent avec des prestataires chargés de les assister dans leur démarche de sécurisation de leurs systèmes. Ces services peuvent être de nature intellectuelle (audit de la sécurité du système d'information, traitement d'incident de sécurité, notamment) ou technique (mécanisme de détection, externalisation, infogérance, mise dans le nuage de tout ou partie du système d'information, tierce maintenance applicative, etc.) ;
- au facteur humain : la sensibilisation du personnel aux questions de sécurité est primordiale, ainsi que la formation de ceux qui interviennent plus spécifiquement dans la mise en œuvre et le suivi opérationnel de la sécurité du système d'information (surveillance, détection, prévention).

D'une manière générale, il est recommandé de s'appuyer sur les guides et sur la documentation produits par l'ANSSI.

Chapitre 2. Description des étapes de la mise en conformité

2.1 Analyse des risques

L'analyse de risques précise les besoins de sécurité du système d'information en fonction de la menace et des enjeux.

La démarche d'analyse de risques consiste à identifier les évènements qui peuvent affecter la sécurité du système, d'en estimer les conséquences et les impacts potentiels puis de décider des actions à réaliser afin de réduire le risque à un niveau acceptable.

Les menaces[1] à prendre en compte sont celles qui pèsent réellement sur le système et sur les informations qu'il traite, transmet et stocke, dans l'environnement dans lequel il se situe.

Lorsque le système d'information intègre des certificats électroniques ou de l'horodatage électronique, l'analyse des risques doit permettre de décider des usages (signature, authentification, confidentialité, etc.) et des niveaux de sécurité (*, ** ou ***) qui seront mis en œuvre.

Il est recommandé de s'appuyer sur la norme ISO 27005, qui fixe un cadre théorique de la gestion des risques. Sa mise en œuvre pratique peut être facilitée par les explications et les outils, notamment logiciels, proposés par la méthode *Expression des besoins et indentification des objectifs de sécurité* (EBIOS).

2.2 Définition des objectifs de sécurité

Une fois les risques appréciés, l'autorité administrative doit énoncer les objectifs de sécurité à satisfaire. Aux trois grands domaines traditionnels (disponibilité et intégrité des données et du système, confidentialité des données et des éléments critiques du système) peuvent s'ajouter deux domaines complémentaires :

- l'authentification, afin de garantir que la personne identifiée est effectivement celle qu'elle prétend être ;
- la traçabilité, afin de pouvoir associer les actions sur les données et les processus aux personnes effectivement connectées au système et ainsi permettre de déceler toute action ou tentative d'action illégitime.

Les objectifs de sécurité doivent être exprimés aussi bien en termes de protection que de défense des systèmes d'information. Les autorités administratives peuvent s'appuyer sur le guide méthodologique EBIOS 2010, afin de formuler précisément ces objectifs de sécurité.

2.3 Choix et mise en œuvre des mesures de sécurité adaptées

L'expression des objectifs de sécurité permet d'apprécier les fonctions de sécurité qui peuvent être mises en œuvre pour les atteindre (art. 3, al. 3 du décret RGS). Ces fonctions de sécurité sont matérialisées par le choix de moyens et de mesures de nature :

- technique : produits de sécurité (matériels ou logiciels), prestations de services de confiance informatiques ou autres dispositifs de sécurité (blindage, détecteur d'intrusion...) ;
- organisationnelle : organisation des responsabilités (habilitation du personnel, contrôle des accès, protection physique des éléments sensibles...), gestion des ressources humaines (affectation d'agents responsables de la gestion du système d'information, formation du personnel spécialisé, sensibilisation des utilisateurs).

[1] Une menace est considérée par le ISO/CEI Guide 73 : 2002 comme une « cause potentielle d'un incident indésirable, pouvant entrainer des dommages au sein d'un système et d'un organisme ».

Ces mesures de sécurité peuvent être sélectionnées au sein des référentiels et normes existants. Elles peuvent également en être adaptées ou bien être créées *ex nihilo*.

2.4 Homologation de sécurité du système d'information

Les systèmes d'information qui entrent dans le champ de l'ordonnance du 8 décembre 2005 doivent faire l'objet, avant leur mise en service opérationnelle, d'une décision d'homologation de sécurité.

Egalement dénommée « attestation formelle » (art. 5, al. 1 du décret RGS), elle est prononcée par une *autorité d'homologation*, désignée par la ou les autorités administratives chargées du système d'information[2].

La décision d'homologation atteste, au nom de l'autorité administrative, que le système d'information est protégé conformément aux objectifs de sécurité fixés et que les risques résiduels sont acceptés. La décision d'homologation s'appuie sur un dossier d'homologation. Lorqu'elle concerne un téléservice, cette décision est rendue accessible aux usagers.

Il est recommandé que les systèmes d'information homologués fassent l'objet d'une revue périodique.

Afin d'homologuer leurs systèmes d'information, les autorités administratives peuvent utiliser les recommandations décrites dans le guide publié par l'ANSSI [Guide homologation].

2.5 Suivi opérationnel de la sécurité du système d'information

Les mesures de protection d'un système d'information doivent être accompagnées d'un suivi opérationnel quotidien ainsi que de mesures de surveillance et de détection, afin de réagir au plus vite aux incidents de sécurité et de les traiter au mieux.

Le suivi opérationnel consiste à collecter et à analyser les journaux d'évènements et les alarmes, à mener des audits réguliers, à appliquer des mesures correctives après un audit ou un incident, à mettre en œuvre une chaîne d'alerte en cas d'intrusion supposée ou avérée sur le système, à gérer les droits d'accès des utilisateurs, à assurer une veille sur les menaces et les vulnérabilités, à entretenir des plans de continuité et de reprise d'activité, à sensibiliser le personnel et à gérer les crises lorsqu'elles surviennent.

(...)

[2] Elle diffère de l'homologation prononcée sur le fondement de l'IGI 1300 pour les systèmes d'informations traitant des informations classifiées de défense.

DOCUMENT 10
« Méthode AGILE : définition, étapes et exemples » - Everlaab - 2022

Si vous vous intéressez à la gestion de projet, vous avez forcément déjà entendu parler de la **méthode Agile**. Cette méthode s'est beaucoup popularisée au cours de ces dernières années. Et pour cause, elle permet de s'adapter rapidement aux changements, ce qui est indispensable dans un monde qui va très vite.

Aujourd'hui beaucoup d'entreprises travaillent en mode Agile notamment Apple, IBM, Microsoft ou encore Procter & Gamble.

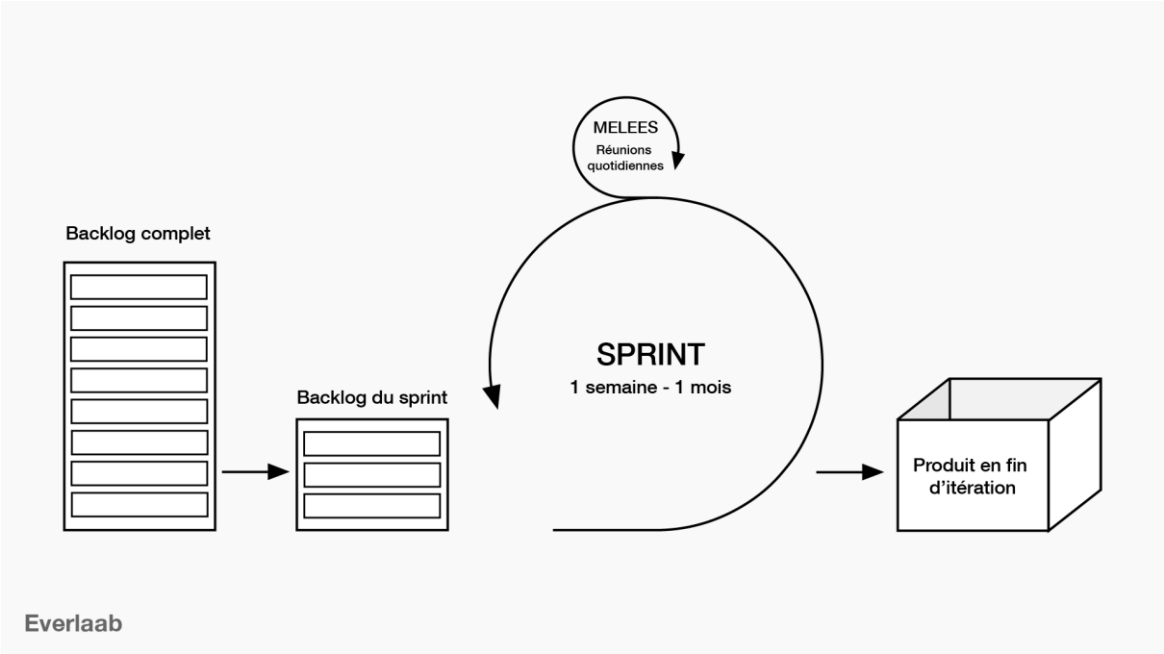
Alors qu'est-ce que la méthode Agile ? Quels sont ses avantages et inconvénients ? Et comment l'appliquer étape par étape ?

Méthode Agile : définition

La **méthode Agile** est une méthode de gestion de projet qui consiste à décomposer vos projets en une suite de petits objectifs atteignables.

Cette approche a été développée dans les années 2000 par 17 ingénieurs américains qui étaient insatisfaits des méthodes de gestion de projet de l'époque et qui leur reprochaient d'être trop lourdes, lentes et contraignantes.

Quand vous travaillez en mode Agile, vous travaillez en de petits cycles courts que l'on appelle sprints ou itérations qui durent généralement entre 1 semaine et 1 mois. On est donc bien loin des méthodes traditionnelles du type diagramme de Gantt ou des méthodes en cascade qui consistent à définir des plans de projet sur 12 ou 24 mois.



Il existe plusieurs façons d'appliquer la méthodologie Agile. Vous pouvez utiliser la méthode Kanban, Scrum ou encore l'extreme programming (XP). Toutes ces méthodes ont été construites sur les bases du **Manifeste Agile**.

Le Manifeste Agile

Le **Manifeste Agile** est un document qui a été écrit dans les années 2000 pour codifier la méthodologie Agile. Ce Manifeste s'axe autour de 4 valeurs :

- **Les individus et leurs interactions** plutôt que les processus et les outils
- **Des logiciels opérationnels** plutôt qu'une documentation exhaustive
- **La collaboration avec les clients** plutôt que la négociation contractuelle
- **L'adaptation au changement** plutôt que le suivi d'un plan

Méthode Agile : avantages et inconvénients

Les avantages de la méthode Agile

La méthode Agile présente de nombreux avantages :

- **Flexibilité** : Avec l'approche Agile, vous travaillez en flux tendu. Vous vous occupez des tâches qui sont importantes à un instant T. Vous êtes donc capable de vous adapter rapidement à votre environnement.
- **Feedback** : La notion de feedback est au cœur de la méthodologie Agile. À la fin de chaque sprint, vous livrez votre travail et récupérez les feedbacks de vos clients ou de vos utilisateurs puis vous les incorporez dans le sprint suivant ce qui permet de coller au plus près à leurs besoins.
- **Compétitivité** : Quand vous travaillez en mode Agile, vous livrez régulièrement de nouvelles fonctionnalités, de nouveaux produits et de nouvelles améliorations ce qui vous rend compétitif et attractif auprès de vos clients et utilisateurs.
- **Qualité** : La livraison fréquente de projets, les tests et l'intégration permanente de feedbacks permettent de développer un produit final de qualité. Pendant tout le cycle de production, le produit est testé et confronté à la réalité.

Les inconvénients de la méthode Agile

L'approche Agile a aussi quelques inconvénients :

- **Manque de documentation** : Étant donné que le scope des projets change au gré des besoins et des feedbacks, il est difficile de tenir une documentation à jour. La documentation d'un produit Agile est donc généralement moins travaillée et détaillée.
- **Gestion des demandes** : Intégrer continuellement les demandes des clients et utilisateurs vous rend plus réactif, mais cela implique aussi de devoir gérer un plus grand volume de demandes entrantes ce qui peut compliquer la gestion de projet.
- **Manque de prévisibilité** : Quand vous travaillez en mode Agile, vous ne savez pas toujours à quoi ressemblera le résultat final. Difficile donc de prévoir le coût, le temps et les ressources nécessaires.

Maintenant que vous connaissez les tenants et les aboutissants de la méthode Agile, comment la mettre en oeuvre concrètement ?

Dans la partie suivante, vous allez découvrir comment appliquer l'approche Agile avec la **méthode Scrum**.

Les étapes de la méthode Agile Scrum

Scrum est une des méthodes Agile les plus populaires. Elle définit 3 rôles au sein des équipes :

- **Le Product Owner** qui réalise la vision du projet, c'est lui qui est chargé de maintenir le backlog à jour (le backlog est l'inventaire des tâches à réaliser).
- **Le Scrum Master** qui est garant de la méthodologie Scrum. Il n'a pas le rôle de chef de projet. Il est chargé de promouvoir la méthode Scrum et de s'assurer qu'elle est bien comprise et utilisée.
- **L'équipe qui réalise le projet**. Elle peut inclure différents types de personnes : des développeurs, graphistes, ingénieurs…

Voici les étapes de la méthode Agile Scrum.

Étape 1 : Définissez le cadre du projet

Pour commencer, définissez le cadre du projet c'est-à-dire l'objectif du projet et ses différentes exigences.

Prenons un exemple simple pour bien comprendre. Admettons que vous soyez ébéniste et que vous vouliez créer une nouvelle gamme de meubles pour votre boutique. Votre objectif pourrait être "*Créer une nouvelle gamme de meubles en bois*" et vos exigences "*Limiter le coût de fabrication à 250€ par meuble*."

Étape 2 : Préparez le backlog

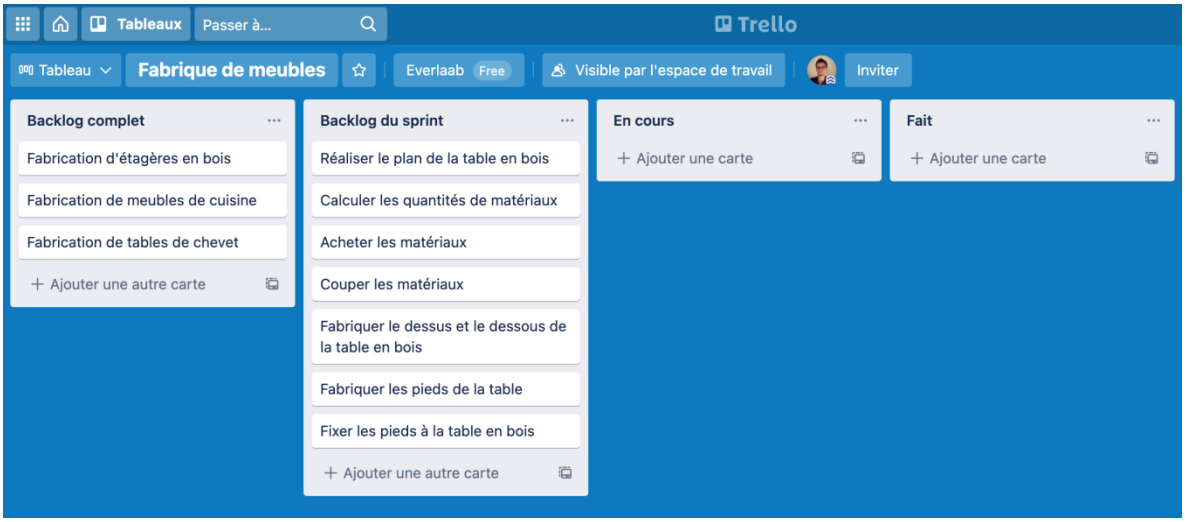
Une fois que vous avez défini le cadre de votre projet, préparez votre backlog. Autrement dit, listez l'ensemble des actions à réaliser pour atteindre votre objectif final et priorisez-les. Au moment de faire cet exercice, gardez bien en tête le cadre du projet, mais aussi les exigences de vos clients.

Si vous êtes ébéniste, il s'agira de prendre en considération les retours de vos clients pour coller au plus près à leur besoin. Peut-être qu'en discutant avec eux, vous remarquerez que certains recherchent des meubles spécifiques. Peut-être que 40% d'entre eux veulent acheter des tables rondes, 30% des étagères, 20% des meubles de cuisine et 10% des tables de chevet.

En gardant ces informations en tête, vous serez capable de les prioriser et de choisir sur quoi vous concentrer pendant toute la durée du sprint.

D'après les données que vous avez récoltées, vous devez vous concentrer sur la fabrication de tables rondes étant donné que la demande est plus forte pour ce type de produit.

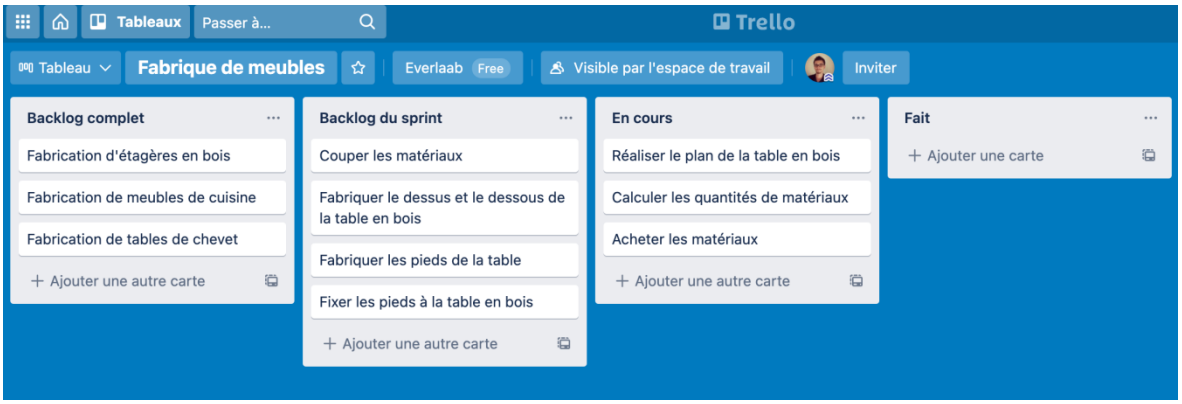
Vous pouvez présenter toutes ces données dans un tableau Trello comme celui-ci :



Dans la colonne *Backlog complet*, vous ajoutez toutes les demandes et besoins de vos clients. Et dans la colonne *Backlog du sprint*, vous indiquez les tâches sur lesquelles vous allez travailler pendant le sprint. Ici comme ce sont les tables rondes qui sont les plus demandées, vous décomposez cette demande en une succession de tâches.

Étape 3 : Travaillez sur les tâches de votre sprint

Maintenant que vous avez défini les tâches de votre backlog, il est temps de travailler sur chacune d'entre elles pendant toute la durée du sprint.



Pour rappel, les sprints sont des cycles courts de travail intense qui durent généralement entre 1 semaine et 1 mois. Le but étant d'avoir quelque chose de présentable à proposer à la fin de chaque sprint.

Si vous travaillez sur la fabrication d'une table ronde, vous devrez donc avoir un modèle de table à présenter en magasin à la fin de votre sprint.

Pendant le sprint, vous devez aussi organiser ce que l'on appelle des mêlées ou scrum en anglais. Les mêlées sont les réunions quotidiennes de 15 min pendant lesquelles les membres de votre équipe expliquent les tâches qu'ils ont terminées depuis la dernière mêlée, celles qu'ils feront lors de la prochaine mêlée et quels sont les obstacles qu'ils rencontrent.

Ces courtes réunions quotidiennes permettent de synchroniser les efforts de l'équipe et de lever les potentiels blocages pendant la réalisation des projets.

Étape 4 : Récoltez les feedbacks

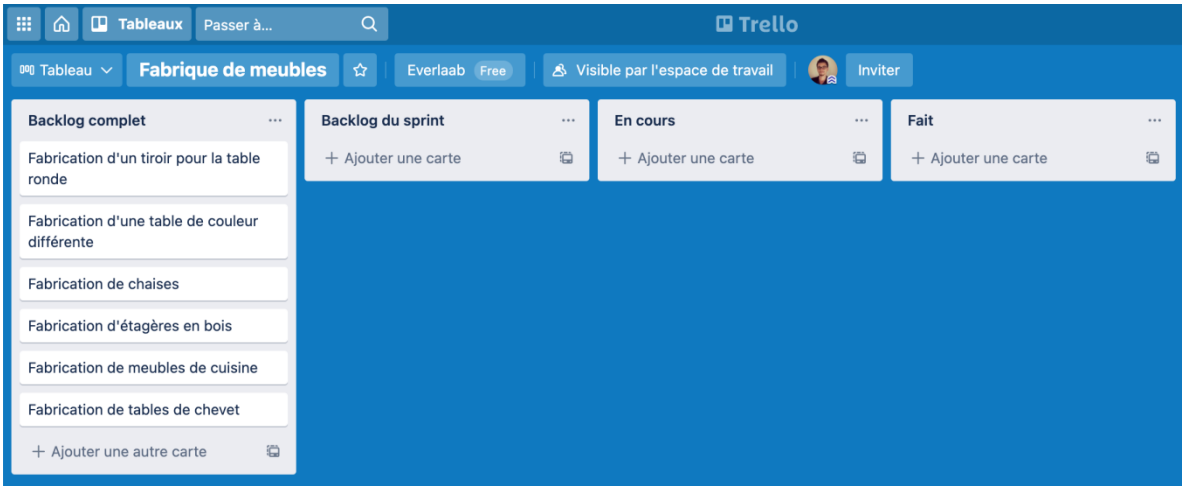
À la fin de chaque sprint, faites une **revue de sprint**. Pendant cette revue, récoltez un maximum de feedbacks auprès de vos clients ou utilisateurs.

C'est à ce moment-là que vous présentez votre table en magasin et que vous demandez aux personnes qui viennent dans votre boutique ce qu'elles en pensent.

Quels sont les aspects qu'elles aiment de la table ? Qu'est-ce qu'elles n'aiment pas ? Qu'est-ce qu'elles voudraient que la table ait en plus ?

Peut-être que certaines personnes vous diront qu'elles aimeraient que la table ait un tiroir, d'autres qu'elle soit d'une couleur différente et d'autres encore qu'elles aimeraient pouvoir acheter des chaises assorties.

Prenez des notes et ajoutez-les dans la colonne *Backlog complet*. Ces demandes détermineront les tâches sur lesquelles vous travaillerez lors de vos futurs sprints.



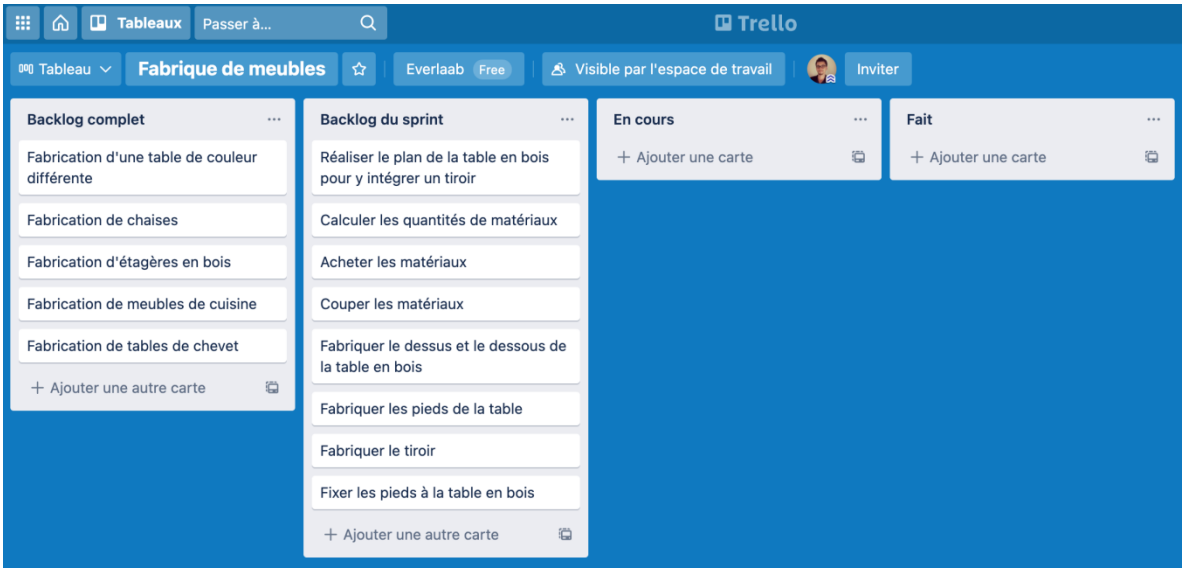
Profitez-en aussi pour faire une rétrospective de votre sprint. Faites un point sur le travail qui a été accompli. Regardez ce qui s'est bien passé, ce qui s'est moins bien passé et tirez-en des leçons. Le but ici est de vous améliorer en continu.

Étape 5 : Recommencez

Après avoir récolté les feedbacks de vos clients et utilisateurs, recommencez le processus. Regardez dans la colonne *Backlog complet* toutes les demandes que l'on vous a faites et déterminez celles qui sont prioritaires.

Transférez-les ensuite dans la colonne *Backlog du sprint* et listez les différentes tâches que vous devez accomplir pour les traiter.

Si fabriquer une table avec un tiroir est prioritaire, transférez la demande dans la colonne Backlog du sprint et listez les différentes tâches que vous devez accomplir pour la traiter.



Travaillez sur ces tâches pendant un sprint. À la fin du sprint, récoltez des feedbacks. Ajoutez-les dans votre backlog et recommencez.

En suivant ces étapes, vous avancerez sur vos projets en mode Agile.

Conclusion

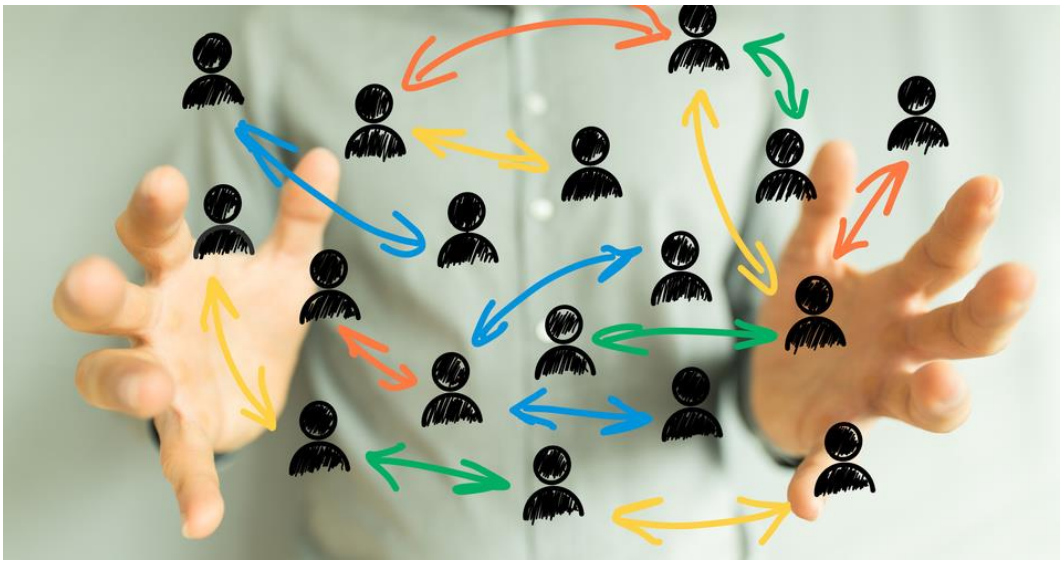
La méthode Agile est une méthode de gestion de projet qui consiste à décomposer vos projets en une suite de petits objectifs atteignables et sur lesquels vous travaillez lors de sprints.

Il existe plusieurs façons d'appliquer la philosophie Agile : la méthode Kanban, Kanban, Scrum ou encore l'extreme programming (XP).

Voici les étapes à suivre pour appliquer la méthode Agile Scrum :

- **Étape 1** : Définissez le cadre du projet en lisant les objectifs et exigences
- **Étape 2** : Préparez le backlog en listant toutes les demandes de vos clients/utilisateurs
- **Étape 3** : Travaillez sur les tâches de votre sprint
- **Étape 4** : Récoltez les feedbacks de vos clients/utilisateur
- **Étape 5** : Recommencez

DOCUMENT 11
« BRM, la courroie de transmission entre la DSI et les métiers » - blog-orsys.fr - 10 février 2017



Relationship

Avec la révolution numérique en cours, les entreprises traditionnelles basculent dans un nouveau monde. Celui mené par de nouveaux acteurs, les GAFA, Airbnb et autres Uber… Leur existence même est parfois remise en cause. Cette transformation spectaculaire change les rapports de la DSI à son organisation. Quel est donc le rôle des business relationship manager (BRM) dans cette transformation ?

La DSI était jusqu'ici trop souvent « technocentrée ». Par nécessité étant donnée la complexité croissante des systèmes informatiques, ou car l'entreprise l'avait cantonnée à un rôle purement technique.

Le Cloud la libère d'un certain nombre de contraintes. Jusqu'ici statique, l'infrastructure devient dynamique et programmable. Elle est capable de s'adapter de manière instantanée à la charge de travail**. Ce changement de paradigme permet aux DSI de se focaliser sur l'optimisation des services et non plus sur le hardware.**

Avec la blockchain, les robots intelligents ou les plateformes d'intermédiation, l'écosystème numérique est, par ailleurs, devenu si complexe qu'il est indispensable pour assurer leur maîtrise de renforcer les processus de gouvernance. Ces innovations doivent s'aligner sur le système d'information et trouver leur cohérence dans la stratégie globale de l'entreprise.

Le BRM : un partenaire stratégique et tactique des métiers

C'est dans cette nouvelle donne que s'inscrit **le Business Relationship Manager (BRM) en tant que go-between entre les fournisseurs de technologies, la DSI, et**

les business units. Par le passé, certaines DSI avaient mis en place des correspondants clients chez les métiers pour capter les besoins.

Pour **Henri Puissant*,** consultant en organisation, management et systèmes d'Information, CEO de la société I-T&S, et formateur chez ORSYS, le rôle du BRM va plus loin puisque son rôle consiste à maximiser la production de valeur. «*Après avoir bien compris la stratégie des business units, le BRM identifie les changements dans l'environnement du client et les tendances technologiques qui potentiellement pourraient impacter le type, le niveau ou l'utilisation des services fournis. »*

Le BRM va identifier les opportunités et les risques puis les intégrer à la stratégie de l'entreprise. Pour cela, il doit donc établir et maintenir une relation constructive entre la DSI et la business unit. *« Son rôle ne se limite plus à capter des exigences, il doit être un véritable partenaire stratégique et tactique des métiers* », poursuit Henri Puissant.

« Cette véritable révolution culturelle vient remettre en cause nos pratiques latines forgées de longue date par la loi MOP (Maîtrise d'Ouvrage Publique) », avance Henri Puissant tout en soulignant que la transformation sera progressive. Créé en 2013, le BRM Institute établit ainsi cinq niveaux de maturité : ad hoc, order taker, service partner, trusted advisor, strategic partner.

Le BRM participe au marketing relationnel de la DSI

Marketing relationnel

Pour Henri Puissant, le rôle du BRM ne doit pas être confondu avec celui du Chief Digital Officer. « *Par définition, le CDO n'est là que pour deux ou trois ans, le temps d'impulser la transition numérique. La fonction de BRM est, quant à elle, pérennisée*

au sein de la DSI. Elle y œuvre en permanence à l'adaptation de l'entreprise à son écosystème. »

Si le BRM travaille en étroite collaboration avec les business units, il n'en est pas moins rattaché à la DSI. Et ce, afin de garantir une bonne gouvernance de l'architecture de l'entreprise*. « Avocat des business units au sein de la DSI, il assure une bonne compréhension des stratégies et tactiques de l'entreprise*, complète Henri Puissant. *Au niveau opérationnel, il est un facilitateur pour régler les problèmes. »*

Pour être bien comprise, l'introduction d'un BRM doit être vue comme **le déploiement d'un marketing relationnel de la DSI au sein de l'entreprise**. *« Pour la DSI, il ne s'agit plus de fournir un service sur commande mais de créer des conditions de relations d'échanges, fondées sur la fidélité mutuelle et la confiance entre un fournisseur et son client.* Objectif : contribuer à la maximisation de la création de valeur pour l'entreprise. »

Un mouton à cinq pattes

Et donc quel profil pour être BRM ? Le BRM doit, selon Henri Puissant, réunir un bouquet de compétences, relationnelles, managériales – prospective et stratégie, architecture de l'entreprise, analyse de la valeur… – et personnelles – capacité d'abstraction et d'analyse, aptitude à travailler en équipe…

Sa connaissance profonde de l'entreprise et de son écosystème lui permet donc de saisir les enjeux du moment*.* « *Le poste peut être occupé par un cadre, informaticien qui a une bonne connaissance du métier ou inversement interlocuteur métier maîtrisant la technologie et ses tendances* », estime-t-il. Le périmètre exact de son poste est défini par le référentiel ITIL® v3-2011 et la norme ISO 20 000.

Enfin, si le phénomène est arrivé plus vite dans les pays anglo-saxons, quelques entreprises pionnières ont mis ou mettent en place ce poste en France comme La Mutuelle Générale ou le cabinet Mazars.

Le RGS : une bonne opportunité pour faire de la sécurité au sein des collectivités locales ?

Dans les esprits, le respect du RGS (Référentiel Général de Sécurité) est souvent cantonné à la mise en oeuvre de certificats électroniques SSL "étoilés". Dans la réalité, il dépasse ce périmètre technique en adressant de bonnes pratiques d'organisation et de gestion de la sécurité.

Au-delà du pur objectif normatif voire légal, quels bénéfices peut-on tirer de la mise en oeuvre d'une démarche d'homologation RGS ?

Tout d'abord, il nous semble important de démystifier le RGS.

Le RGS, en vrai c'est quoi ?

Adopter une approche par les risques : Adapter la démarche et le niveau de sécurité cible en fonction des risques et du contexte.

Formaliser une politique de sécurité globale : Formaliser le cadre général de la sécurité intégrant les objectifs de sécurité de l'organisation, la description des rôles et des responsabilités (MOA, RSSI, Comités, ...) liés à la sécurité et les principes fondamentaux.

Intégrer la sécurité dans la vie du SI et dans les projets : Se poser les bonnes questions le plus tôt possible pour éviter de mal y répondre voire de ne pas y répondre du tout.
Souvent impossibilité de prendre le temps d'atteindre le niveau cible avant la publication car la promotion du nouveau télé-service est déjà lancée auprès des usagers.
Parfois incapacité d'atteindre le niveau cible car les exigences n'ont pas été inclues dans le CCTP et donc non respectées par le prestataire en charge de la fourniture de la solution.

Utiliser des produits et des prestataires labellisés : Un "coup de tampon" d'un tiers de référence sur un service ou une solution, c'est un gage de qualité et de confiance pour renforcer la démarche sécurité.

Mettre en place un processus d'homologation : Un représentant de la collectivité, appelé Autorité d'Homologation (AH), doit attester formellement, en s'appuyant sur un Dossier de Sécurité, que le niveau de sécurité de l'application est conforme au niveau cible attendu.

Quels bénéfices pour la collectivité et la fonction sécurité ?

Le RGS représente une réelle opportunité pour faire de la sécurité et apporter de la valeur à la collectivité et à la fonction sécurité en :

Accompagnant le développement de la dématérialisation et des services innovants des villes et territoires "intelligents".

Engageant une collaboration pérenne autour de la sécurité de l'information entre des Fonctions qui ont souvent du mal à communiquer (et manquent d'occasion de le faire), c'est-à-dire la Communication (TIC, Numérique, ...), le Juridique et l'Informatique, et même entre le RSSI et les autres Services au sein de la Direction Informatique.

Sensibilisant la Direction, les agents et même les usagers vis-à-vis des risques liés à la cybercriminalité et aux nouveaux usages.

Contribuant à l'acculturation au concept de gestion des risques et ainsi à l'amélioration de l'image du RSSI qui est souvent vu comme "celui qui bloque" plutôt que "celui qui encadre les usages".

Comment s'y prendre ? Nos 5 règles d'Or

Règle n°1 : Obtenir l'adhésion

Comme pour toute démarche transverse, il est indispensable, afin qu'elle aboutisse, d'obtenir l'adhésion de la Direction et des représentants des Fonctions "Communication/Numérique", "Juridique" et "Informatique" (bien sûr).

Tout un programme...

C'est ici que le RGS, en tant que référentiel imposé par l'ANSSI et faisant écho à la Loi Informatique et Libertés bien connue de tous (le mot-clé "CNIL" résonne plutôt bien), permet plus facilement (ou pour être plus réaliste, moins difficilement), de fédérer diverses fonctions autour d'une démarche Sécurité.

Règle n°2 : S'assurer que la règle n°1 est bien respectée

Etre sûr que la règle n°1 sera respectée en s'appuyant sur vos relais internes (Correspondant Informatique et Libertés, Chargé de Mission e-administration, DGA, ...) au moyen de quelques sessions de présentation du RGS et de ses bénéfices pour la collectivité.

En fonction de votre organisation (et des possibilités offertes), identifier qui sera votre Autorité d'Homologation : Elu référent informatique, DGS, DGa, ...

Règle n°3 : Identifier les applications soumises au RGS

Réaliser un inventaire des applications soumises au RGS déjà et à venir.

Règle n°4 : Intégrer de la sécurité dans les projets

Définir, en collaboration avec les équipes projet technique et étude, une démarche d'intégration de la sécurité dans les projets (ISP) s'appliquant aux projets RGS et également aux autres projets (c'est-à-dire la grande majorité cf règle n°3). Intégrer dans la démarche ISP un volet Analyse de risques pragmatique et généralisable.

Règle n°5 : Expérimenter sur un projet pilote

Expérimenter la démarche sur un ou deux projets pilotes en choisissant un projet "phare" pour faciliter la règle n°1.

Ce qu'il faut en retenir

Le RGS, plus qu'une simple obligation, permet de donner une véritable impulsion dans la démarche globale de sécurité et de fédérer différentes Directions au sein de la collectivité. Avec une démarche pragmatique, la mise en oeuvre est tout à fait possible.

ANNEXE 1
« Présentation générale du Système d'Information d'INGEDEP » - *INGEDEP* -
Novembre 2021

Le Conseil Départemental d'INGEDEP est doté d'un réseau étendu de 130 sites interconnectés. On recense aujourd'hui 400 serveurs physiques et / ou virtuels au sein du datacenter de la collectivité. Les 47 collèges du département sont interconnectés avec le réseau d'INGEDEP et font partie des 130 sites.

La collectivité a déployé largement depuis 2015 une solution de virtualisation du poste de travail et cela lui a permis de bien s'adapter à l'expansion du télétravail durant la crise sanitaire. Le nombre de postes de travail est de 2 000 qui se répartissent ainsi :

- 1 200 clients légers (box) dans le cadre de la virtualisation des postes de travail,
- 600 portables pour les agents en situation de mobilité,
- 200 PC fixes pour les usages non éligibles à la virtualisation

Au sein d'INGEDEP, la Direction des Systèmes d'Information et des Services Numériques (DSISN) est composée de 40 agents dont une majorité d'ingénieurs territoriaux. Elle assure la gestion des infrastructures, des applications et des projets ainsi que le développement et le maintien en condition opérationnelle du Système d'Information.

Le SI comprend de nombreuses applications transversales (gestion financière, gestion des ressources humaines, gestion des délibérations ...) et des applications dédiées aux compétences de la collectivité (aide sociale, routes, laboratoire,...).

Toutes les ressources sont hébergées en interne, les équipes de la DSISN maîtrisent l'ensemble des composants du système d'information et le recours au Cloud est rare. De multiples applications contiennent des données personnelles notamment les applications du secteur social. Le délégué à la protection des données et le RSSI sont positionnés au sein de la Direction Générale, il n'existe pas de procédures formalisées afin de les intégrer de manière systèmatique dans le déroulement des projets. Des actions de communication sont parfois menées sur l'intranet de la collectivité pour expliquer aux agents les raisons de la mise en œuvre de certaines contraintes (par exemple le changement régulier des mots de passe).

Le Conseil Départemental d'INGEDEP est équipé d'une solution libre de messagerie d'entreprise basée sur la solution Zimbra. Cette solution donne satisfaction et permet d'offrir les services suivants :

- Envoi / réception de messages en interne et en externe
- client Web
- Accès par login/mot de passe à la messagerie depuis internet pour tous les utilisateurs (depuis la crise sanitaire).

La solution bureautique "Libre Office" est déployée sur tous les postes de travail (physiques et virtuels). Microsoft Office est parfois installé, uniquement pour les applications qui le nécessitent.

La collaboration autour des projets avec les acteurs internes et externes se fait grâce à la messagerie en l'absence d'autres outils collaboratifs.