Chambre régionale des comptes
Bretagne

RAPPORT D'OBSERVATIONS DÉFINITIVES ET SA RÉPONSE

DÉPARTEMENT DU MORBIHAN
Gestion des systèmes d'information

Exercices 2016 et suivants

Le présent document, qui a fait l'objet d'une contradiction avec les destinataires concernés, a été délibéré par la chambre le 25 mai 2023.

Chambre régionale des comptes Bretagne
3, rue Robert d'Arbrissel
35042 RENNES CEDEX

TABLE DES MATIERES

SYNTHÈSE

Le système d'information (SI) est un ensemble complexe de ressources de natures diverses (ressources humaines, matériels principalement informatiques, logiciels), destiné au traitement d'informations. Sa gestion connait de profonds bouleversements depuis plusieurs années avec la dématérialisation des métiers et des traitements de dossiers mais aussi, plus encore depuis la crise sanitaire, avec le développement du télétravail. Dans un contexte de moyens financiers contraints et de risques accrus en termes de sécurité, le département se doit de disposer de réseaux et systèmes performants et d'optimiser et de préserver leur sécurité.

Une gouvernance des systèmes d'information dont l'amélioration est à poursuivre

Le département a fait réaliser en 2019 un audit externe, mettant en avant une insatisfaction des agents à l'égard de leurs logiciels métiers, une direction des systèmes d'information (DSI) insuffisamment orientée vers le service aux utilisateurs, sa communication interne et externe perfectible, ainsi qu'une insuffisante maîtrise de la gestion des projets pour pouvoir accompagner efficacement la transition numérique du département.

Depuis lors, le département a amélioré la gouvernance de sa DSI avec des outils de pilotage satisfaisants et la mise en œuvre d'une méthodologie de gestion des projets permettant une meilleure prise en charge des demandes des directions. Ces évolutions sont intervenues dans un contexte de progression des budgets consacrés à la politique numérique départementale : la collectivité a ainsi consacré 1,08 % de ses dépenses de gestion pour le seul fonctionnement de ses SI en 2021 (contre 1 % en 2016), soit un niveau supérieur à la moyenne des autres départements (0,83 %). De même, de 2016 à 2021 le département a investi 16,7 M€ dans ses SI.

Le département a également réuni au sein d'une même direction générale la direction des ressources humaines et la DSI devenue direction des services numériques (DSN). Ce changement d'organisation vise à mieux accompagner des services dans la conduite du changement. Néanmoins, faute d'adoption d'un schéma stratégique priorisant les projets et les actions, le département s'inscrit dans des arbitrages au fil de l'eau en fonction des moyens disponibles. La gouvernance des SI doit donc encore être consolidée avec l'adoption de documents stratégiques et d'outils offrant une meilleure connaissance des risques et des relations entre les applications métiers. Cette nouvelle étape apparaît indispensable pour que la collectivité puisse passer d'une logique de moyens à une logique d'objectifs.

Une gestion des données à améliorer

Si le département a rapidement pris en charge les obligations qui lui incombent en matière de recensement de ses activités de traitement des données personnelles, en application du règlement général sur la protection des données (RGPD), il lui reste à compléter le recensement de ses activités de traitement et leur inscription dans son registre.

Il n'a par ailleurs pas encore adopté de politique de confidentialité des données recueillies sur son site Internet et que peu investi le champ des données ouvertes. Il n'a ainsi mis en ligne sur *data.gouv.fr* que 20 jeux de données, parfois anciennes. Outre le fait qu'une telle démarche s'impose à lui en vertu de l'article L. 312-1-1 du code des relations entre le public et l'administration, il est rappelé que la réutilisation des données mises à disposition offre de nouveaux services aux citoyens et peut constituer un levier d'amélioration de la définition des politiques publiques.

Des pistes de rationalisation à expertiser afin d'optimiser la gestion du SI départemental

Les modes d'organisation et de gestion actuels pourraient être optimisés en favorisant des rationalisations départementales, notamment avec le service départemental d'incendie et de secours et la maison départementale de l'autonomie, mais également interdépartementales (projets de développement et de déploiement d'applications informatiques ou de gestion de données communes, recrutement mutualisé de personnels spécialisés tels que des *data analysts* ou *scientists*).

RECOMMANDATIONS

Sur le fondement des observations du rapport, la chambre formule les recommandations et rappels au respect des lois et règlements suivants :

Les recommandations et rappels au respect des lois et règlements formulés ci-dessus ne sont fondés que sur une partie des observations émises par la chambre. Les destinataires du présent rapport sont donc invités à tenir compte des recommandations, mais aussi de l'ensemble des observations détaillées par ailleurs dans le corps du rapport et dans son résumé.

Il est par ailleurs rappelé que l'article L. 243-9 du code des juridictions financières pose l'obligation, dans un délai d'un an à compter de la présentation du rapport d'observations définitives à l'assemblée délibérante, de présenter, dans un rapport de suites, les actions entreprises à la suite des recommandations mais aussi de l'ensemble des observations de la chambre.

INTRODUCTION

Procédure

La chambre régionale des comptes Bretagne a procédé, dans le cadre de son programme de travail, au contrôle des comptes et à l'examen de la gestion du département du Morbihan à compter de l'exercice 2016. Ce contrôle a été ouvert par lettres du 3 mars 2022 adressées à MM. François Goulard, ancien président et David Lappartient, président.

L'entretien de début de contrôle s'est déroulé le 20 avril 2022 avec M. Lappartient. L'entretien de fin de contrôle prévu par l'article L. 243-1 du code des juridictions financières a eu lieu le 22 septembre 2022 avec M. Goulard et le 30 septembre 2022 avec M. Lappartient.

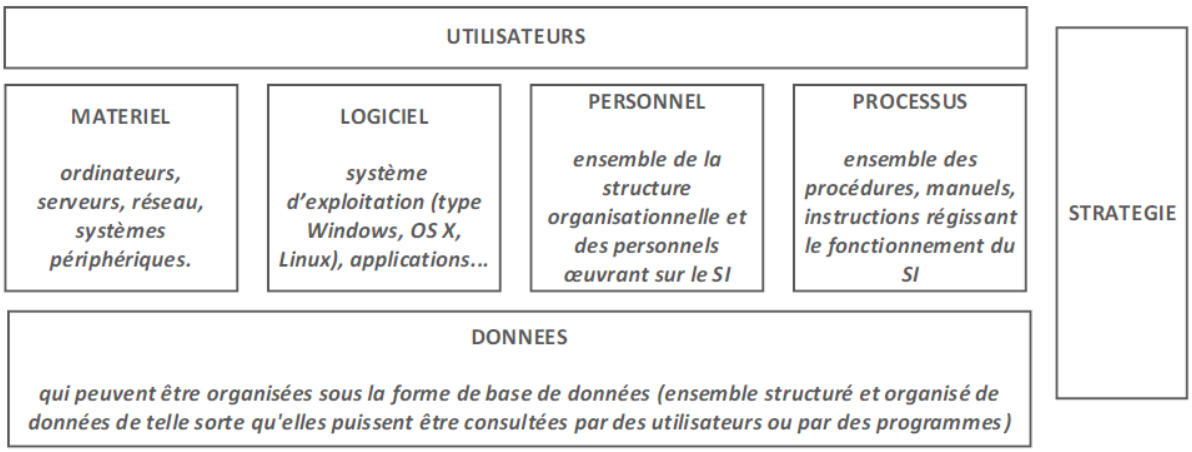
La chambre, lors de sa séance du 30 novembre 2022, a arrêté ses observations provisoires qui ont été adressées le 4 avril 2023 à MM. Goulard et Lappartient. La réponse de M. Lappartient est parvenue à la chambre le 25 avril 2023. M. Goulard n'a pas apporté de réponse.

Après avoir examiné la réponse reçue, la chambre, lors de sa séance du 25 mai 2023, a arrêté ses observations définitives.

1 UN ENVIRONNEMENT EN PLEIN BOULEVERSEMENT

Un système d'information (SI) est un ensemble complexe de ressources de natures diverses (ressources humaines, matériels principalement informatiques, logiciels) avec comme matière première des données et comme résultat des informations.

Schéma n° 1 : Les briques des systèmes d'information



Source : guide d'audit des SI – Cour des comptes.

Les logiciels et outils informatiques ne sont donc qu'une partie des composantes d'un SI. Celui-ci occupe une place stratégique et se trouve au cœur du fonctionnement de toute collectivité. La qualité, l'intégrité et la sécurité du système d'information conditionnent aujourd'hui l'efficacité de l'action de l'administration, face au développement des attaques et des risques informatiques[1].

1.1 Des attaques en augmentation

En 2020, la commission nationale de l'informatique et des libertés (Cnil) a reçu 144 notifications à la suite de piratages, logiciels malveillants (par exemple rançongiciels) et hameçonnages concernant les administrations publiques, contre 78 en 2019. Les principales attaques subies par les collectivités sont le défaçage (intrusion sur le site internet pour en modifier le contenu), les rançongiciels (chiffrement des données assorti d'une demande de rançon) et les chevaux de Troie (ouverture d'une porte dans l'infrastructure pour permettre une utilisation frauduleuse).

[1] https://www.amf.asso.fr/m/document/fichier.php?FTP=3346071583bfb5c73b7c9ec2f265bf66.pdf&id=40484https://www.ccomptes.fr/fr.

Les conséquences de ces attaques peuvent être lourdes. Une commune d'Ile-de-France, cible d'un rançongiciel, a ainsi perdu l'ensemble de ses systèmes et données en l'absence de sauvegarde externe, malgré la présence de deux serveurs redondants touchés par l'attaque. Dès lors, elle a été dans l'incapacité d'utiliser l'ensemble des applications métiers, des mails et des outils nécessaires à la facturation ou au recouvrement des recettes. La commune n'a pu donc établir ses paies, ses comptes et procéder au paiement de ses fournisseurs pendant une longue période. Cette situation a entrainé d'importantes surcharges de travail dans les équipes. Des départements ont subi des vols de bases de données et reçu des menaces visant à diffuser en ligne des données personnelles.

1.2 Le nomadisme

La crise sanitaire a contraint les entreprises et administrations à s'adapter rapidement au travail à distance mais également à définir et mettre en place les mesures nécessaires à cette nouvelle organisation du travail. Elles se sont heurtées à l'absence de solutions logicielles sur lesquelles s'appuyer, ainsi qu'au manque de matériel physique pour doter leurs collaborateurs d'outils de télétravail, tandis que les principaux incidents rencontrés étaient liés à la capacité et à la performance des infrastructures réseau disponibles.

Cette modification des modes d'organisation s'est accompagnée de risques liés à l'utilisation de solutions logicielles, dont l'assurance en termes de confidentialité pouvait être mise en doute.

1.3 La digitalisation des métiers

Engagées dans une mutation de l'environnement de travail, les entreprises et administrations sont amenées à accompagner la digitalisation des métiers, ce qui place les directions des systèmes d'information (DSI) au cœur du changement. Cette digitalisation des métiers implique que les DSI se forment à leurs spécificités pour fournir les solutions les plus adaptées aux besoins.

La transformation numérique est également une réalité et un enjeu majeur pour les collectivités territoriales. La multiplication de l'utilisation des technologies numériques transforme le fonctionnement du service public et la relation à l'usager, notamment par la généralisation des services en ligne et des téléprocédures, mais aussi au regard de l'optimisation de l'analyse des données de masse et de l'utilisation de l'intelligence artificielle. Le développement du télétravail dans les collectivités a par ailleurs imposé l'adaptation des moyens informatiques à ces nouvelles conditions de travail.

Dans un contexte de moyens financiers contraints et de demande sociale en augmentation, les départements sont confrontés à la nécessité d'optimiser leurs moyens de fonctionnement. Cette optimisation passe par la mise en place d'un SI permettant de déployer efficacement de nouveaux outils numériques, de développer et simplifier l'accessibilité aux services publics, d'améliorer les conditions de travail des agents tout en protégeant son intégrité et en renforçant sa sécurité.

2 LA GOUVERNANCE DES SYSTEMES D'INFORMATION : STRATEGIE, ORGANISATION ET GESTION DES RESSOURCES

2.1 L'organisation de la direction des services numériques

2.1.1 L'audit externe de 2019

Afin d'être accompagné dans la transition numérique de son action publique, le département a confié en 2019 la réalisation d'un audit sur l'organisation de sa fonction informatique à un cabinet extérieur.

2.1.1.1 Une direction devant progresser et se structurer en matière de gestion de projets

L'audit pointait tout d'abord le fait que l'absence prolongée de directeur depuis 2016 avait été préjudiciable à la déclinaison des orientations stratégiques de la collectivité et à la définition d'une organisation associée. Plus globalement, il relevait une gouvernance marquée par une démarche ITIL[2] insuffisamment orientée vers le service aux utilisateurs, un service système d'information géographique (SIG) sous-dimensionné et ne pouvant répondre aux besoins des directions métiers, ainsi que des échanges internes insuffisants entre les différents pôles.

En matière de gestion des projets, il était également relevé que la définition des besoins était imprécise, avec un accompagnement insuffisant dans le domaine de l'assistance à la maîtrise d'ouvrage (AMOA) pour traduire les besoins en projets informatiques. Le suivi des projets était en outre réalisé de manière artisanale, via de simples tableurs. L'organisation ne permettait pas non plus de prendre correctement en compte les nouveaux besoins des directions métiers, en raison d'un déséquilibre entre les fonctions techniques et les fonctions métiers. Le diagnostic notait ainsi le manque de maturité dans la méthodologie de la gestion des projets, mais également l'absence de priorisation et l'explosion du nombre de projets avec une implication tardive de la DSI dans ceux-ci, ainsi qu'un manque de dialogue entre la maîtrise d'ouvrage (MOA) et la maîtrise d'œuvre (MOE).

Par ailleurs, le diagnostic faisait ressortir une fréquence élevée des pannes dans les directions, notamment en matière de coupures réseaux, confortée par le nombre d'équivalents temps plein déclarés pour la gestion des incidents techniques, un accès au SI problématique et chronophage sur les sites distants, notamment pour les centres routiers de la direction des routes (DRA) et les sites des centres sociaux (DGISS). De même, les développements spécifiques représentaient par la suite une charge de maintenance importante pour les équipes de la DSI.

Enfin, le diagnostic soulignait l'affectation de ressources insuffisantes pour la veille technologique et le développement des infrastructures techniques du SI (0,45 ETP).

[2] ITIL (pour *Information Technology Infrastructure Library*) : ensemble d'ouvrages recensant les bonnes pratiques du management des SI.

2.1.1.2 Des outils insatisfaisants pour les services utilisateurs

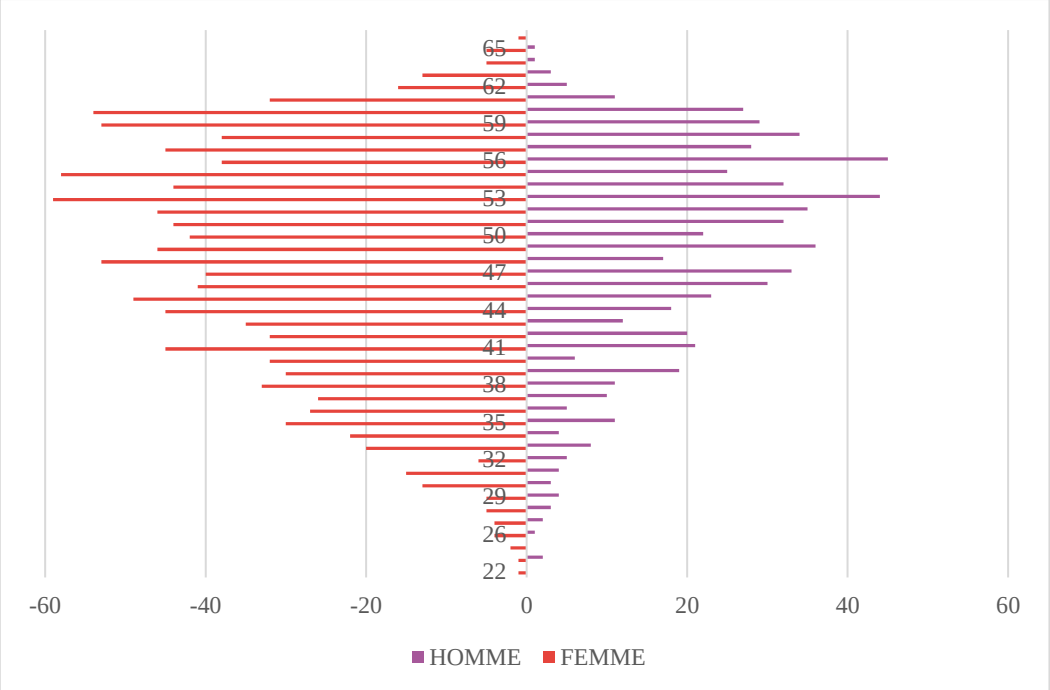
L'audit relevait que les outils métiers étaient à l'origine de nombreuses insatisfactions des directions et services, telles que la DRA (applications vieillissantes peu ou pas utilisées, matériel de mobilité et matériel d'impression inadaptés), la DRH (applications insatisfaisantes), la DGISS (réserves sur l'outil métier et les relations avec l'éditeur, SharePoint peu apprécié, car probablement mal maîtrisé). En outre, certaines applications métiers n'intégraient pas nativement des processus dématérialisés.

Plus globalement, de nombreux développements spécifiques ont été réalisés par la collectivité (30 formulaires, 80 sites intranet, internet et extranet), afin de pallier les insuffisances des applications en termes d'interface et de dématérialisation des processus et la mauvaise qualité des relations avec les éditeurs. Ils ont toutefois entraîné une saturation de la charge des équipes études. De même, la plupart des formulaires développés ne permet pas d'intégrer automatiquement les données dans l'application métier, ce qui donne lieu à des ressaisies qui sont source d'erreurs.

En outre, l'audit alertait la collectivité sur les outils d'archivage et de partage de documents, en raison du recours à des espaces réseaux qui ne constituent pas une solution sécurisée et efficiente.

Enfin, la pyramide des âges de la collectivité peut refléter une moindre appétence pour les outils numériques d'une partie des agents, en dehors même de cultures métiers marquées par une méfiance vis-à-vis de l'outil numérique.

Graphique n° 1 : Pyramide des âges au 31 décembre 2019



Source : CRC à partir des fichiers de paie.

2.1.2 Impliquer la direction des systèmes d'information dans la conduite du changement en matière numérique

La direction des systèmes d'information (DSI), devenue direction des services numériques (DSN), fait partie de la direction générale adjointe (DGA) des ressources humaines et numériques (DGRHN), qui comprend également la direction des ressources humaines (DRH), une chargée de communication interne, un conseiller en organisation et le médecin de prévention. Cette organisation mise en place en avril 2020 répond à la volonté d'accompagner les évolutions numériques et de faire de la nouvelle direction un partenaire des services dans la conduite du changement. Le conseiller en organisation permet de réaliser des cartographies de processus métiers, étape utile pour déployer de nouveaux logiciels.

Si le rattachement à la direction générale de directions opérationnelles telles que les directions des routes et des collèges présente l'avantage d'un circuit de décision plus court, il peut également conduire à une saturation au niveau de la direction générale à qui remonte l'ensemble des informations, pour le pilotage des projets transversaux et, à terme, à un cloisonnement des directions. À cet égard, le regroupement de la DRH et de la DSN au sein de la DGRHN peut permettre d'articuler les politiques de conduite du changement et la formation et ainsi faciliter la modernisation du management. Cette organisation doit néanmoins s'accompagner d'une stratégie de conduite du changement qu'il convient de définir et de piloter.

La chambre recommande de compléter la réorganisation ayant conduit à réunir la DRH et la DSN au sein de la DGRHN, par un plan de conduite de la transformation numérique. En réponse aux observations provisoires, le département a indiqué travailler sur les besoins métiers avec une prise en compte des enjeux de mobilité et des moyens associés. En outre, un nouveau plan de formation serait lancé en 2023 afin d'accompagner les agents dans la transformation numérique de leurs métiers.

Recommandation n° 1 Se doter d'un plan de conduite de la transformation numérique prévoyant la gouvernance et les moyens confiés à la DGRHN.

Enfin, le rapprochement de la DSN et de la DRH au sein de la DGRHN facilite la rationalisation de la gestion des identités et comptes utilisateurs, qui constitue un axe indispensable dans la sécurisation du réseau.

2.1.3 L'organigramme de la DSN

2.1.3.1 Un recentrage de l'activité vers les directions métiers

Une réorganisation a eu lieu en avril 2020 à la suite du recrutement d'un nouveau directeur, avec pour axe principal le regroupement des compétences et une plus grande ouverture vers les directions métiers pour la prise en compte de leurs demandes.

L'organigramme s'articule désormais autour de trois services et un pôle : le service études, le service ingénierie, le service support aux usagers du numérique et le pôle missions aménagement numérique et information géographique. À cette occasion, l'organisation a davantage été tournée vers l'utilisateur que la dimension technique/réseaux, ce qui répond aux préconisations de l'audit de 2019.

2.1.3.2 Les tableaux de bord de la direction

La direction dispose de tableaux de bord concernant le suivi des projets. La DSN est dotée désormais d'un logiciel de gestion de projets paramétré pour intégrer la gestion des demandes et la gestion du portefeuille de projets et actions. De même, le centre de services supports établit un rapport d'activité mensuel facilitant le pilotage de la direction, avec la communication d'informations utiles aux services chargés de l'aménagement du réseau et études.

2.2 La stratégie et la gouvernance

2.2.1 L'absence de schéma directeur des systèmes d'information

La collectivité ne s'est pas dotée d'un schéma directeur des systèmes d'information (SDSI).

Un SDSI est un document central dans la gouvernance des SI et son absence constitue une faiblesse majeure pour le pilotage de la collectivité. Ainsi, le Cobit[3] insiste sur le fait qu'un plan informatique stratégique permet à la DSI d'une entité de mieux piloter son budget et d'avoir une vision globale des investissements à moyen et long termes. La DSN doit donc être en mesure de réagir aux exigences métier, en accord avec la stratégie métier, et aux exigences de la gouvernance, en accord avec les orientations du conseil d'administration de l'entité.

La chambre recommande à la collectivité de se doter dès 2023 d'un SDSI reposant sur un diagnostic de l'existant et comportant une définition des besoins et des enjeux, aux plans organisationnel, fonctionnel, applicatif, technique et réglementaire. À partir des orientations et de l'identification des différents scénarios, ce document devra prévoir un plan d'action.

[3] *Control OBjectives for Information and related Technology* (Cobit) : résultat des travaux collectifs réalisés par les principaux acteurs de la profession, auditeurs internes ou externes, fédérés au sein de l'*Information system audit and control association* (Isaca), association mondiale basée aux États-Unis et présente dans les plus grandes villes du monde. Elle est représentée en France par l'Association française pour l'audit et du conseil en informatique (AFAI). Dans ses premières versions publiées à partir de 1996, Cobit se positionne comme un référentiel de contrôle. Il décline sur le domaine IT les principes du référentiel *Committee of sponsoring organizations of the treadway commission* (COSO), publiés pour la première fois en 1992 et dont l'objectif est d'aider les entreprises à évaluer et à améliorer leur système de contrôle interne.

Recommandation n° 2 Arrêter un schéma directeur des systèmes d'information conforme aux normes professionnelles Cobit, afin de garantir dans le temps la cohérence d'ensemble du système d'information et son adéquation aux besoins de la collectivité.

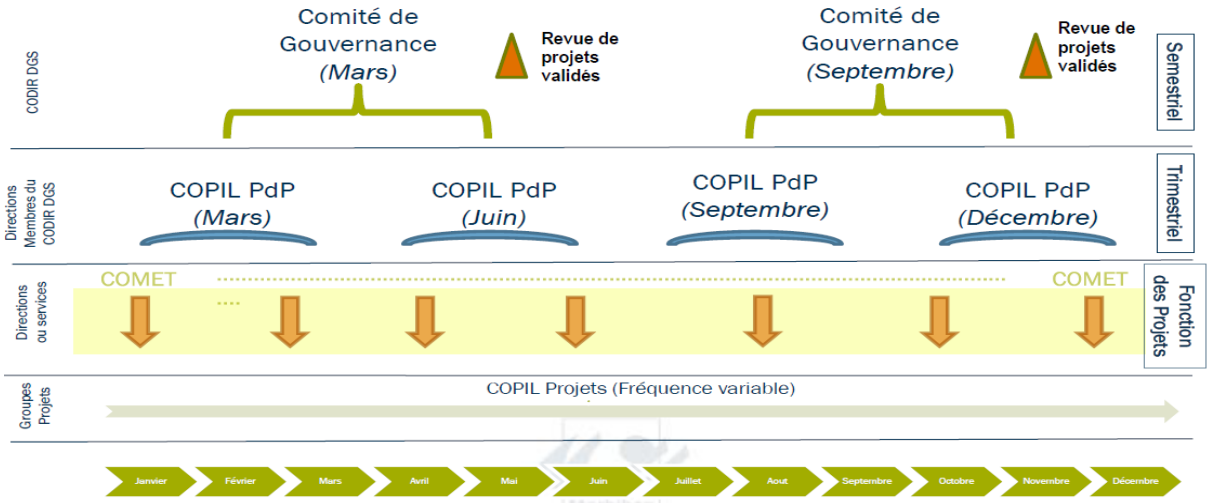
2.2.2 Les instances de gouvernance

Une nouvelle organisation appelée « comitologie » a été mise en place début 2020 et déployée complètement un an plus tard afin de suivre l'ensemble des demandes faites à la DSN. Elle comprend :

- la mise en place d'une collaboration entre la DSN (en qualité de référent maîtrise d'ouvrage - RMOA) et les directions métiers (en qualité d'assistants à maîtrise d'ouvrage - AMOA) ;
- l'organisation de la chefferie des projets ;
- la mise en place d'un comité métier (COMET) entre la DSN et les directions au sein des directions générales ;
- la mise en place de « comités de pilotage de portefeuille de projets » entre la DSN et les directions générales membres du comité de direction de la direction générale des services (Codir DGS) ;
- la mise en place d'un « comité de gouvernance » de validation semestrielle de projets, avec une priorisation des nouveaux projets de toutes les directions générales en lien avec les ressources disponibles côté DSN et dans les directions métiers.

Ce dernier comité est réuni tous les six mois et constitue le point central de la gouvernance des projets numériques de la collectivité. Si le schéma de comitologie reproduit ci-dessous ne mentionne pas les membres des différents comités, il est néanmoins orienté à partir des niveaux de priorité identifiés et en tenant compte du budget agents disponible après affectation des projets de maintien en condition opérationnelle (MCO) et des projets en cours.

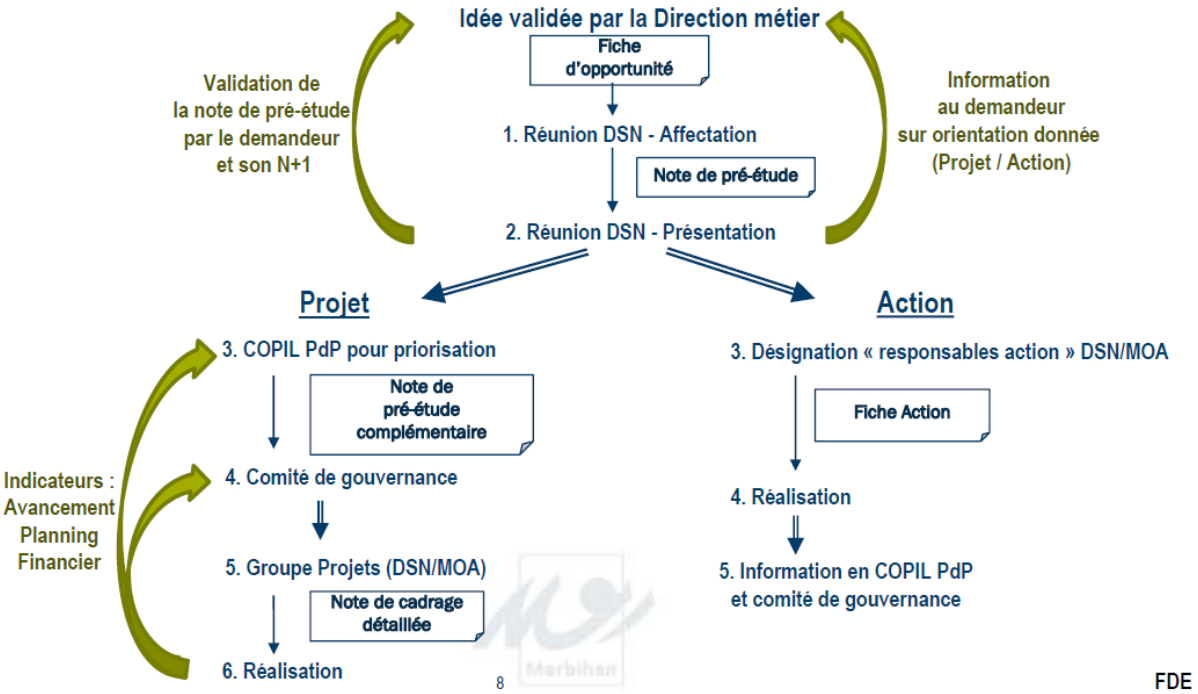
Schéma n° 2 : La gouvernance des comités de pilotage



Source : département.

Le comité de gouvernance répond aux attentes du référentiel Cobit[4].

Schéma n° 3 : Le circuit de validation des projets



Source : département.

La procédure retenue, en l'absence de dimension pluriannuelle, peut toutefois conduire à écarter des projets sensibles faute de budget, ceux lancés absorbant déjà une part importante des ressources. La mise sur pied de ce comité ne saurait donc dispenser le département de l'élaboration d'un schéma directeur.

2.3 La gestion des projets : une conformité aux standards à poursuivre et à formaliser

Si la collectivité a institué un binôme chef de projet numérique/chef de projet fonctionnel, conformément aux normes relatives aux bonnes pratiques définies par le Cobit s'agissant des comités de pilotage[5], il est relevé qu'aucune documentation de la méthode projet n'a toutefois été arrêtée.

[4] « Le comité stratégique informatique est rattaché au plus haut niveau de l'entreprise. Il s'assure de la bonne gouvernance du SI et conseille la direction de l'entreprise dans les orientations stratégiques et les choix d'investissement informatique en fonction des besoins des métiers. Selon la taille et la criticité de l'entreprise, il est présidé par le président de l'entreprise ou un directeur général délégué. »

[5] Il est composé de cadres représentant les métiers et l'informatique afin de mettre en œuvre la stratégie informatique définie par la direction de l'entreprise. Il assure le pilotage des investissements informatiques et des activités de service (priorités/arbitrages, résolution des conflits d'accès aux ressources).

Ces normes prescrivent par ailleurs la mise en place d'un comité des utilisateurs, afin d'arrêter l'expression détaillée des besoins et des règles de gestion, de valider les dossiers de conception présentés par l'équipe projet, de participer aux tests du système, à l'élaboration de la documentation « utilisateurs », aux actions de formation et de réceptionner définitivement le logiciel. Ce comité des utilisateurs n'étant pas prévu par le département, les chances de réussite des principaux projets transversaux s'en trouvent affaiblies.

En outre, le département n'a pas non plus déployé de documents types (études d'opportunité, lettres de mission, cahiers des charges, fiche d'évaluation du projet, etc.) permettant de s'assurer d'une expression détaillée des besoins par la MOA et d'une méthodologie standard. En leur absence, il prend le risque d'un manque d'homogénéité des méthodes et livrables.

Néanmoins, la gestion des projets de refonte du système d'information sur les ressources humaines (SIRH) et du logiciel financier a permis de constater l'existence de procès-verbaux des comités de pilotage, l'association des principaux services concernés, ainsi que la désignation d'un chef de projet métier et d'un chef de projet informatique pour chaque projet.

Au vu de ces constats, la chambre invite le département à mieux formaliser la gestion des projets en établissant des documents-types afin de garantir une uniformisation de la gestion de l'ensemble des projets.

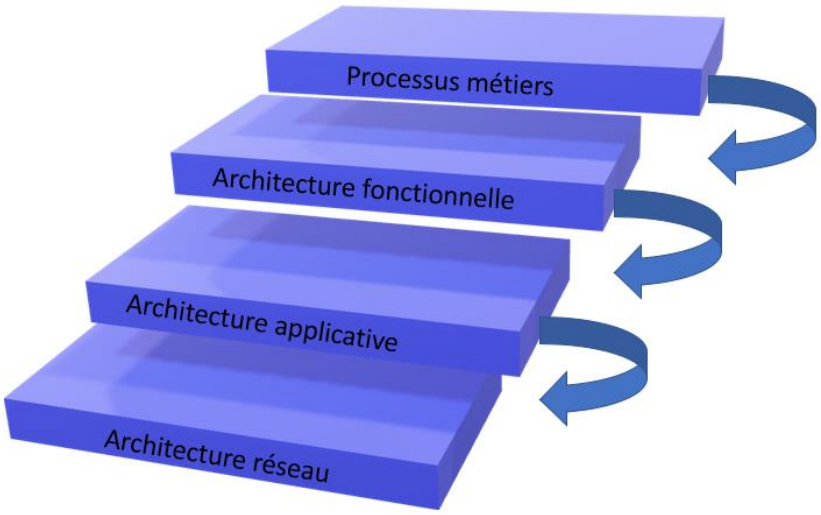
2.4 Un outil de pilotage des systèmes d'information à conforter : la cartographie

Dans un contexte numérique, la cartographie permet de représenter le SI d'une organisation ainsi que ses connexions avec l'extérieur. Cette représentation plus ou moins détaillée peut, par exemple, inclure les matériels, les logiciels, les réseaux de connexion, mais aussi les informations, les activités et les processus. La cartographie doit ainsi permettre de réaliser l'inventaire patrimonial du SI (liste et description détaillée des composants) et présenter visuellement ses liens et son fonctionnement, afin de rendre lisibles et compréhensibles ses différents aspects.

De manière générale, la cartographie est composée de trois visions allant progressivement du métier vers la technique, elles-mêmes déclinées en vues :

- vision métier : représentation du SI à travers ses processus et informations principales (valeurs métier au sens de la méthode d'appréciation des risques *EBIOS Risk Manager*) ;
- vision fonctionnelle : description de la structuration du système d'information en blocs fonctionnels communicants (fonctions permettant de supporter les processus métiers) ;
- vision applicative : description des composants logiciels du SI, des services qu'ils offrent et des flux de données entre eux. La vue de l'administration répertorie les périmètres et les niveaux de privilèges des utilisateurs et des administrateurs ;
- vision infrastructure : description des équipements physiques composant le SI ou utilisés par celui-ci.

Schéma n° 4 : Les différents niveaux de cartographie



Source : CRC.

2.4.1 La cartographie applicative

Le département ne dispose pas de cartographie applicative, alors même qu'il s'agit d'un élément indispensable à toute politique d'urbanisation[6] des SI.

La cartographie des applications, en présentant les interfaces entre applications, les éventuelles utilisations d'outils bureautiques pour des transferts de données et les relations avec les entités extérieures (comme c'est par exemple le cas avec l'application Helios), permet de mettre en évidence les risques potentiels liés à l'architecture générale des applications. Elle permet également de réagir plus efficacement en cas d'incident ou d'attaque numérique, de qualifier les impacts et de prévoir les conséquences des actions défensives réalisées. Cette cartographie aide par ailleurs à identifier les activités clés de l'organisme, afin de définir un plan de continuité d'activité et s'impose comme un outil indispensable à la gestion de crise, qu'elle soit numérique ou non.

Elle s'accompagne généralement d'une cartographie de criticité des outils informatiques, afin d'identifier les systèmes les plus critiques et les plus exposés, d'anticiper les chemins d'attaque possibles sur ces systèmes et de mettre en place des mesures adéquates pour assurer leur protection. Le département ne s'est pas non plus doté d'une telle cartographie.

Elle constitue enfin un outil de rationalisation du travail quotidien des agents, en permettant par exemple de repérer les interfaces manquantes afin d'éviter les doubles saisies ou les risques liés à des saisies sous tableurs, ainsi que les applications redondantes.

[6] « L'urbanisation des systèmes d'information désigne le processus de transformation des systèmes d'information vers une architecture modulaire permettant une meilleure maîtrise de leur complexité. Par extension, une gestion urbanistique des systèmes d'information caractérise la présence de règles et les structures de gestion des systèmes d'information, inspirées des règles et structures d'urbanisme, permettant d'assurer la constitution et pérennisation de cette architecture modulaire. » Marc Bidan, Cécile Godé, *Management des systèmes d'information,* Cairn Info, septembre 2022. https://www.cairn.info/dscg-5-management-des-systemes-d-information--9782311404357-page-51.htm.

En l'absence de cartographie applicative, le département n'est pas en mesure de faire évoluer son urbanisation applicative. La chambre recommande au département de se doter d'une telle cartographie.

En réponse aux observations provisoires, le département a indiqué qu'un projet de mise en place d'un logiciel spécifique de cartographie applicative était en cours d'étude, reconnaissant qu'il s'agissait d'un travail indispensable à mener sur plusieurs années.

Recommandation n° 3 Établir la cartographie applicative des systèmes d'information.

L'exemple du SIRH

Le département du Morbihan a commandé un audit de son SIRH en 2019[7], afin de poser un diagnostic sur son utilisation interne, d'en tirer le meilleur usage et de l'adapter aux missions de la direction générale adjointe des RH (DGARH).

L'audit a mis en avant l'existence d'une mutitude d'outils au sein de la DGARH[8], non interfacés entre eux et dont la maitrise par les agents est incomplète. Cette situation a conduit à la mise en place par les agents de solutions pragmatiques pour réaliser les missions demandées (utilisation de tableurs), qui sont sources d'erreurs dans le traitement des données à l'échelle d'un département[9].

L'audit relève également un retard en matière de dématérialisation. Celle-ci gagnerait à être développée via des formulaire dématérialisés (congés, CET, temps partiels…) afin de faire des agents les acteurs de cette transformation.

Enfin, il est noté que plusieurs outils achetés par le département ne répondent pas entièrement aux besoins exprimés, ce qui engendre des erreurs ou des tâches chronophages dans l'utilisation des données, avec à la clé un coût élevé pour la collectivité.

2.4.2 La cartographie des risques

Dans une démarche gloable de maîtrise des risques, il est indispensable qu'une cartographie des risques liés au SI soit élaborée et mise à jour régulièrement et que des contrôles internes soient mis en œuvre pour mitiger les principaux risques.

[7] Analyse et audit du système d'information des ressources humaines effectué par les cabinets C4S et Territoires et technologie de l'information conseil.

[8] Le SIRH était éclaté en six logiciels métiers spécialisés (recrutement, formation, gestion prévisionnelle des emplois et des compétences (GPEC), carrières, paies et gestion des temps et absences).

[9] Par exemple, le logiciel formation ne permet pas d'incrémenter le logiciel GPEC, le logiciel GPEC n'offre pas de bascule vers le logiciel des carrières et des paies et ce dernier ne permet pas de récupérer les données renseignées dans le logiciel des absences.

La cartographie des risques à l'échelle de la collectivité

La collectivité s'est engagée en 2021 dans une démarche de cartographie globale de ses risques en vue de fournir au nouvel exécutif une vision d'ensemble des menaces pesant sur l'institution, de revisiter ses stratégies de traitement des risques et de répondre à certaines obligations réglementaires ou de les anticiper.

Pour contribuer au développement de la culture du risque au sein de la collectivité, la méthode retenue repose sur une approche ascendante (*bottom up*) et déclarative. Chaque direction a ainsi été invitée à recenser et coter les cinq risques majeurs pour son propre périmètre et à identifier les cinq risques majeurs à l'échelle plus large de la collectivité. L'évaluation des risques s'est faite sur la base d'une échelle de criticité et de maîtrise commune.

Les résultats recueillis lors de cette première étape ont fait l'objet d'une première consolidation. Il en est ressorti une prédominance des risques opérationnels, avec un niveau de maîtrise déclaré permettant de les classer majoritairement parmi les risques acceptables, et peu de risques majeurs faisant l'objet d'une maîtrise significativement perfectible.

Une deuxième étape est en cours d'exécution afin d'améliorer la qualification des risques, leur évaluation et leur hiérarchisation. Une vision consolidée et stabilisée était attendue avant la fin de l'année 2022. En réponse aux observations provisoires, le département a indiqué avoir procédé à une réduction du nombre de risques par une cotation plus fine de leur gravité, tout en les ayant rendus plus explicites et mieux à même de faire l'objet d'arbitrages quant aux mesures de traitement à engager.

Si la méthode retenue offre un état des lieux proche de la réalité, elle ne permet pas toujours de relier ces risques à la stratégie de la direction générale. Le nombre limité de risques à identifier par direction et l'absence de cartographie sectorielle a également pu entrainer une cartographie insuffisamment opérationnelle. Les 19 risques recensés en synthèse par le département restent ainsi très généraux et doivent être décomposés en risques plus fins[10]. De même, les mesures de mitigation/remédiation proposées apparaissent trop vagues[11].

La chambre invite le département à décliner la cartographie des risques de la collectivité par des cartographies plus sectorielles. En réponse aux observations provisoires, le département a indiqué avoir engagé en 2023 des travaux portant sur l'articulation entre cette cartographie globale et quatre cartographies plus sectorielles.

[10] Par exemple « Menaces informatiques » et « Défaillance d'un processus informatique » cotés comme très probables et très impactants.
[11] « Respect des consignes de sécurité informatique, MAJ du référentiel de sécurité, sauvegarde ».

2.5 Les mutualisations possibles

2.5.1 La recherche de mutualisations avec les organismes satellites du département

Le département dispose de plusieurs pistes de mutualisation externe pour renforcer l'optimisation de la gestion de ses SI. En effet, s'il assure actuellement tout ou partie de la gestion des SI pour certains de ses satellites (maison départementale de l'autonomie (MDA), ensemble des SI du conseil d'architecture, d'urbanisme et de l'environnement (CAUE), service départemental d'incendie et de secours (SDIS) pour des opérations de câblages et de réseaux), il serait en mesure d'approfondir la mutualisation de ses infrastructures et moyens informatiques et numériques avec ces organismes[12].

À cet égard, même si les spécificités des métiers du SDIS conditionnent les modalités de gestion de leurs SI, ils restent soumis aux mêmes impératifs en termes d'infrastructures (liaison sécurisée multisite, besoins de salles informatiques, achat d'équipements) et doivent disposer de personnels qualifiés (chefs de projets, techniciens), d'un responsable de la sécurité des SI (RSSI) et d'un délégué à la protection des données (DPD).

Le président du conseil départemental est par ailleurs le président du conseil d'administration du SDIS et de la commission exécutive de la MDA. Cette position devrait permettre de renforcer les mutualisations entre ces structures afin d'optimiser la gestion des SI.

2.5.2 La recherche de mutualisation avec les autres départements

L'exemple de la gestion de la maintenance informatique dans les collèges

Conscient des difficultés récurrentes en termes de maintenance informatique dans les collèges et lycées bretons, les quatre départements et la région ont lancé une étude en 2019 afin de disposer de solutions pour assurer la maintenance informatique dans ces établissements. Il s'agissait de déterminer et d'évaluer différentes trajectoires possibles de mutualisation, afin d'améliorer l'organisation de la maintenance informatique. Cette étude a proposé d'analyser quatre scénarios d'organisation portant sur des hypothèses de mutualisation de service plus ou moins renforcées.

Deux expériences ont été analysées dans cette étude : le système mis en place à compter de septembre 2019 en Ille-et-Vilaine en collaboration avec le groupement d'intérêt public santé informatique Bretagne (GIP SIB) et le système en régie mis en place depuis 10 ans à la région. Ce travail a permis au département des Côtes-d'Armor de contracter avec le GIP SIB afin de mettre en place une maintenance externalisée de ses collèges à compter de 2022, comme l'Ille-et-Vilaine et le Morbihan. Le département du Finistère a décidé de ne pas recourir à cette solution.

[12] Une démarche de faisabilité est engagée avec le Centre départemental de l'enfance (CDE).

Les départements sont confrontés à des difficultés similaires portant sur le recrutement de certaines fonctions (chef de projets, cybersécurité) et sur l'absence de taille critique de chacune des collectivités pour peser face à des éditeurs oligopolistiques intervenant sur des marchés de niche (logiciels de gestion sociale, de paie, financier, ressources humaines).

S'il semble difficile d'envisager le recrutement de RSSI ou de DPD mutualisés, compte tenu de l'importance de leur action de proximité auprès des services, une réflexion pourrait être menée sur les modalités de recrutement mutualisé d'un ou plusieurs cadres, afin de piloter un ou des projets de développement et de déploiements d'applications informatiques ou de gestion de données. Ainsi, le recrutement mutualisé de *data analysts* ou *scientists*[13] pourrait être une piste intéressante. Les départements produisent et gèrent d'importants volumes de données qui ne sont pas ou peu exploités à ce jour. Leur analyse affinée permettrait d'améliorer la connaissance des facteurs qui influent sur leurs politiques publiques (liens entre pauvreté, enfance en danger et réussite scolaire…) et la qualité des schémas stratégiques sectoriels. Au surplus, le traitement de la donnée permet d'améliorer la qualité de sa production. Au regard du coût de ce type de recrutement et des volumes de données à traiter, une mutualisation permettrait de réaliser des économies d'échelles.

2.5.3 **Les nécessaires échanges entre les départements**

Les directeurs des SI ont constitué un réseau informel d'échanges qui permet de dialoguer sur les évolutions techniques, l'harmonisation des modes de gestion et l'amélioration des pratiques. De même, les chefs de services disposent de réseaux de correspondants dans les autres départements. Ces réseaux informels s'ajoutent à ceux des clubs utilisateurs des éditeurs ou encore au groupe technique de l'association des départements de France (ADF). Des travaux en commun sont menés : même s'ils restent relativement rares, ils permettent au regard d'un problème commun de disposer d'un diagnostic global et de proposer des solutions et des pistes d'évolution.

La chambre invite la collectivité à mener une réflexion avec les autres départements bretons et, le cas échéant, la région, afin d'expertiser la possibilité de mutualiser les modalités de pilotage de projets de développement et de déploiements d'applications informatiques ou de gestion de données (*data analyst* ou *scientist*).

En réponse aux observations provisoires de la chambre, le département a fait état de la difficulté à mutualiser des postes d'experts spécialistes de la gestion des données, compte tenu des conditions d'attractivité des collectivités. Jugeant plus pertinent un recours à des prestataires externes dans un premier temps, le département s'est toutefois rapproché de l'université de Bretagne Sud, qui porte un important axe de développement sur les sujets numériques. Il a ainsi proposé de recruter des doctorants intéressés par la structuration des données, afin de préfigurer des développements futurs.

[13] Le *data analyst* a pour mission d'exploiter et d'interpréter les données pour en dégager des observations utiles. Ainsi, les rapports fournis permettent d'orienter les prises de décision du management et d'améliorer les performances de la collectivité. Le *data scientist* développe des algorithmes d'apprentissage automatique selon les besoins des équipes métiers. Ses compétences en statistiques lui permettent de construire des modèles de *machine learning* et ses connaissances en informatique l'aident à anticiper leur mise en production. En amont de ces deux missions, il est également chargé de structurer et d'analyser les données qu'il utilise.

3 LA SECURITE DES SYSTEMES D'INFORMATION

Lors de son contrôle, la chambre a procédé à l'examen approfondi de la sécurité des systèmes d'information du département (sécurité externe et interne, plans de continuité et de reprise d'activité, configuration des postes…). En raison de la sensibilité de ces sujets, les observations provisoires s'y rapportant ont été transmises au seul ordonnateur et ne figurent pas dans le présent rapport qui sera rendu public.

3.1 La gouvernance de la politique de sécurité

3.1.1 L'absence de politique de sécurité jusqu'en 2020

Lors du déploiement de son système d'archivage en 2018, le département a réalisé un audit de sécurité. Celui-ci a mis en évidence le fait qu'en matière de sécurité, le département avait une approche principalement cantonnée aux aspects techniques et n'avait pas élaboré de politique stratégique plus large. Or, la sécurité informatique est une démarche partagée qui doit non seulement impliquer la DSI, mais également les utilisateurs.

L'audit estimait en outre que l'absence de responsable de la sécurité des SI (RSSI) et de politique de sécurité des SI (PSSI) entraînait des incohérences dans certains choix architecturaux, des dérives progressives résultant d'habitudes prises au sein des équipes, ainsi que des problèmes liés à des mesures de sécurité non appliquées, simplement parce que les équipes ne se sentaient pas capables de les imposer seules.

3.1.2 La politique de sécurité depuis 2020

La collectivité a arrêté en avril 2021 sa politique générale de SSI (PGSSI), qui a été validée en comité technique. Elle se décline en un corpus documentaire en cours de constitution (politiques opérationnelles de SSI, modes opératoires, procédures, documents d'exploitations) afin de répondre à la norme ISO 27001. Son élaboration a été lancée dès l'arrivée du RSSI dont le poste est rattaché à la direction générale des services, au niveau du service d'audit et d'appui aux politiques publiques. Cette séparation des missions est conforme aux normes en vigueur en la matière. Des objectifs thématiques de PSSI secondaires, intitulés politiques opérationnelles de SSI (POSSI), ont également été arrêtés.

Si les activités du RSSI sont consignées dans une feuille de route en lien avec la stratégie cybersécurité élaborée lors du 2e trimestre 2020, conformément à la PGSSI du département, le nomadisme n'est toutefois pas intégré dans celle-ci comme le préconise pourtant l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La liaison des deux salles serveurs est assurée par deux fibres différentes, ce qui permet un niveau de sécurité élevé, mais engendre également des coûts substantiels. De fait, la PGSSI et les POSSI du département ne définissent pas d'objectifs cibles de sécurité déclinés en moyens à attribuer, ce qui peut entrainer d'éventuelles sur-qualités qui ne sont pas véritablement arbitrées par la direction générale.

En réponse aux observations provisoires, le département a indiqué que depuis 2023, la traduction opérationnelle des politiques de sécurité repose sur une analyse des risques les plus critiques, avec l'établissement de plans d'action soumis à la direction générale.

3.2 La charte informatique

Le département s'est doté d'une charte informatique prenant la forme d'un « règlement intérieur sur l'utilisation des moyens informatiques et de télécommunication » (RIUMIT), dont la dernière version remonte à novembre 2019 et qui est en cours de mise à jour. Diffusé sur l'intranet de la collectivité pour les agents et utilisateurs, il est opposable aux prestataires qui sont assimilés selon le document à des utilisateurs.

Ce document de 20 pages apparaît relativement complet et aborde les principales questions de sécurité. Il ne mentionne toutefois ni le règlement général sur la protection des données (RGPD) et la clause en découlant annexée dans les contrats de marchés pour les sous-traitants, ni l'existence d'un délégué à la protection des données (DPD).

En complément, le département a établi en 2020 un plan d'actions pluriannuel de sensibilisation des agents à la sécurité des SI. Ces actions prennent la forme de messages sur l'intranet et d'interventions en présentiel, dont sont informés les membres du comité directeur de la direction générale des services pour relais managérial auprès des agents du département. Au total, sur les années 2020 et 2021, 12 actions de sensibilisation à destination des agents et des élus ont ainsi été réalisées sur la cybersécurité et 13 notes ont été partagées avec la direction générale des services et le cabinet du président.

3.3 La sécurité logique

La gestion des mots de passe et des accès au SI n'appelle pas d'observation particulière, le département ayant mis en place des procédures d'information de la DSN par la DRH en cas de départs des agents. Seules les mutations internes ne font pas encore l'objet d'une information systématique.

Toutefois, l'analyse de la gestion des droits d'accès aux logiciels de gestion RH (GRH) et de gestion financière fait ressortir plusieurs risques. Le paramétrage des comptes du logiciel de GRH fait apparaître plusieurs caractéristiques telles que la création de 3 292 comptes. Pour le logiciel de gestion financière, 16 utilisateurs disposent de « super-droits » d'administrateurs. Les logs de suivi des accès au logiciel ne sont pas activés pour des raisons de performance.

L'existence d'un grand nombre de comptes administrateurs dont les droits d'accès ne sont pas limités aux responsabilités des agents est porteuse de risques. Ensuite, ces comptes d'administration devraient être exclusivement affectés à des actions d'administration, ce qui devrait se traduire par une séparation des profils utilisateurs et administrateurs avec la création de deux comptes pour ces agents. Tel n'est pas le cas et les actions réalisées en qualité d'administrateur ne font pas l'objet de revues régulières.

La chambre invite le département à restreindre le nombre d'administrateurs, limiter leurs accès à leurs seuls domaines d'intervention, en séparant les identifiants administrateurs de ceux des utilisateurs, et à tracer les actions menées.

3.4 La sécurisation du parc d'ordinateurs

En 2022, l'inventaire du département recense 2 950 postes (dont 1 082 PC, 1 754 portables et 114 tablettes).

Lors du contrôle de la chambre 411 PC fonctionnaient encore sous Windows 7, dont la maintenance « support » a cessé depuis le 15 janvier 2020. Ils ne sont donc plus mis à jour et ne bénéficient plus de support technique. Les bugs et failles de sécurité ne sont donc plus corrigés, tandis que progressivement les applications ne sont plus optimisées pour cette version.

Le département n'a pas arrêté de politique de renouvellement de ses PC, évoquant une priorité pour les ordinateurs sous Windows 7 et un renouvellement dans le cadre de la crise sanitaire et du télétravail. L'âge médian du parc d'ordinateurs qui n'est que de trois ans (quatre ans et quatre mois en moyenne), témoigne cependant de sa faible ancienneté.

En revanche, s'agissant des moyens d'impression, le département compte encore 787 imprimantes pour seulement 167 copieurs. L'audit mené par le département notait que *« Bien que le niveau de satisfaction soit très élevé sur ce thème, le projet sur la rationalisation des moyens d'impression est loin d'être mené à son terme. L'utilisation d'imprimantes individuelles reste trop massive. Le taux d'équipement d'imprimantes et photocopieurs / nbre de postes de travail est de 41,35 %* [alors que la] *Valeur moyenne des Départements : 24 %* ; pour rappel : Coût impression par feuille jet d'encre : 10 à 15 cts ; Coût impression par feuille photocopieur : 3 à 5 cts ».* À cela s'ajoute le fait que l'âge moyen du parc d'imprimantes laser est de 10 ans et six mois. Parallèlement, la DSN a réalisé en 2021 plus de 400 interventions liées à des problèmes d'impressions et d'installations d'imprimantes, tâches couteuses qui pourraient être aisément réduites.

Le retard constaté dans la rationalisation des moyens d'impression est donc patent et devrait conduire la collectivité à y remédier.

En réponse aux observations provisoires, le département a indiqué, d'une part, avoir engagé un chantier de rationalisation de ses systèmes d'édition et, d'autre part, avoir remplacé début 2023 la totalité des anciens PC qui fonctionnaient sous Windows 7.

4 LES MOYENS ALLOUES AU SYSTEME D'INFORMATION

4.1 Les efforts financiers et humains

Avec 1,09 % de ses dépenses de fonctionnement alloués à la fonction informatique en 2017, l'effort financier du département apparaît significatif (0,83 % en moyenne pour les départements bretons).

Il en va de même au plan des moyens humains et matériels, avec un taux d'équipement des agents important, y compris pour les assistants familiaux. Sur ce point, si l'audit externe de 2019 relevait que le taux d'équipement du département (nombre de postes de travail informatiques/effectifs) se situait dans la norme (86,5 % pour une moyenne des départements de 90 %), ce ratio s'établit désormais à 95 %, à la faveur du renouvellement du parc orienté vers des portables et de l'attribution d'outils numériques pour un large panel de métiers, y compris dans le domaine social. Les dépenses de fonctionnement par agent s'élèvent par ailleurs à 2 672 €, soit un niveau supérieur de 18 % à la moyenne régionale. Au total, ces dépenses de fonctionnement représentent 1,04 % des charges de gestion des services du département (hors intérêts et charges exceptionnelles), ce qui les situe également à un niveau supérieur à la moyenne régionale (0,92 %).

Enfin, avec un agent pour 55 postes et 2,85 % des effectifs, la DSN dispose de moyens sensiblement supérieurs à la moyenne bretonne (2,22 %). La proportion d'agents de catégorie A parmi ses effectifs est également supérieure à la moyenne (48 % pour une moyenne régionale de 43 %). De fait, le département a mis l'accent sur ses ressources internes, les dépenses de personnel représentant 60 % de ses dépenses consacrées aux SI, contre une moyenne bretonne de 54 %.

Tableau n° 1 : Les dépenses de fonctionnement consacrées aux SI en 2021

	Charges totales de fonct. (en M€)	*Dont ch. de fonct. hors personnel (en M€)*	*Dont ch. de personnel (en M€)*	*% ch. de fonct.*	*% ch. de personnel*	*Dépenses SI / agent (en €)*
Département 22	4,64	1,67	2,97	35,99 %	64,01 %	1 785
Département 29	6,23	3,58	2,65	57,48 %	42,52 %	2 139
Département 35	8,54	3,9	4,64	45,67 %	54,33 %	2 455
Département 56	5,86	2,37	3,49	40,44 %	59,56 %	2 672
Total	25,532	11,781	13,751	46,14 %	53,86 %	2 258

Source : CRC à partir des données communiquées par les départements.

Si l'attribution de moyens supérieurs à la moyenne des départements témoigne d'un choix politique fort en direction du numérique, celui-ci est freiné par l'absence de documents stratégiques qui prive les élus et la direction générale de leur pouvoir d'arbitrage.

En réponse aux observations provisoires de la chambre, le département a indiqué vouloir compléter sa gouvernance par la réalisation d'un schéma stratégique numérique établissant les grands principes d'évolution du système d'information dans les années à venir.

4.2 **Les dépenses affectées à la direction des systèmes numériques**

Les dépenses de fonctionnement du service, qui s'élèvent en 2021 à 5,9 M€ dont 2,4 M€ de charges à caractère général, ont augmenté de 0,5 M€ depuis 2016, en raison notamment de l'augmentation de la masse salariale. Parmi ces dépenses de fonctionnement, les frais de télécommunication ont augmenté de 0,27 M€, tandis que les frais de maintenance ont pu être réduits de 0,4 M€. Ce dernier poste n'incluant pas la maintenance du logiciel de gestion des ressources humaines dont la garantie court encore l'année suivant son déploiement, il sera amené à augmenter à hauteur de 15 % de la valeur du logiciel. Au total, les dépenses de fonctionnement représentent donc 1 % des charges de gestion. En ajoutant les dépenses d'investissement, les dépenses du service représentent 1,47 % des dépenses réelles en 2021. Leur part a augmenté au cours de la période puisqu'elles se limitaient à 1,09 % en 2017.

Si la crise sanitaire s'est traduite par une diminution des dépenses de fournitures, le département a massivement renouvelé son parc à cette occasion, avec une progression significative des dépenses de matériel informatique (1,85 M€ en 2021 contre 0,78 M€ en moyenne entre 2016 et 2020). Par ailleurs, le département a réalisé d'importantes dépenses de câblage en 2021, notamment en fibre (0,845 M€).

Les dépenses totales (fonctionnement et investissement) de la direction qui s'établissaient à 7,5 M€ par an en moyenne de 2016 à 2019, ont enregistré une forte hausse à partir de 2020 où elles se sont élevées à 8,5 M€. La crise sanitaire s'est en effet accompagnée d'un développement des besoins en matière de mobilité et de sécurité, qui a amené le département à investir en acquisitions de matériels et de licences (près de 0,5 M€[14]). Elles se montent à 10,8 M€ en 2021.

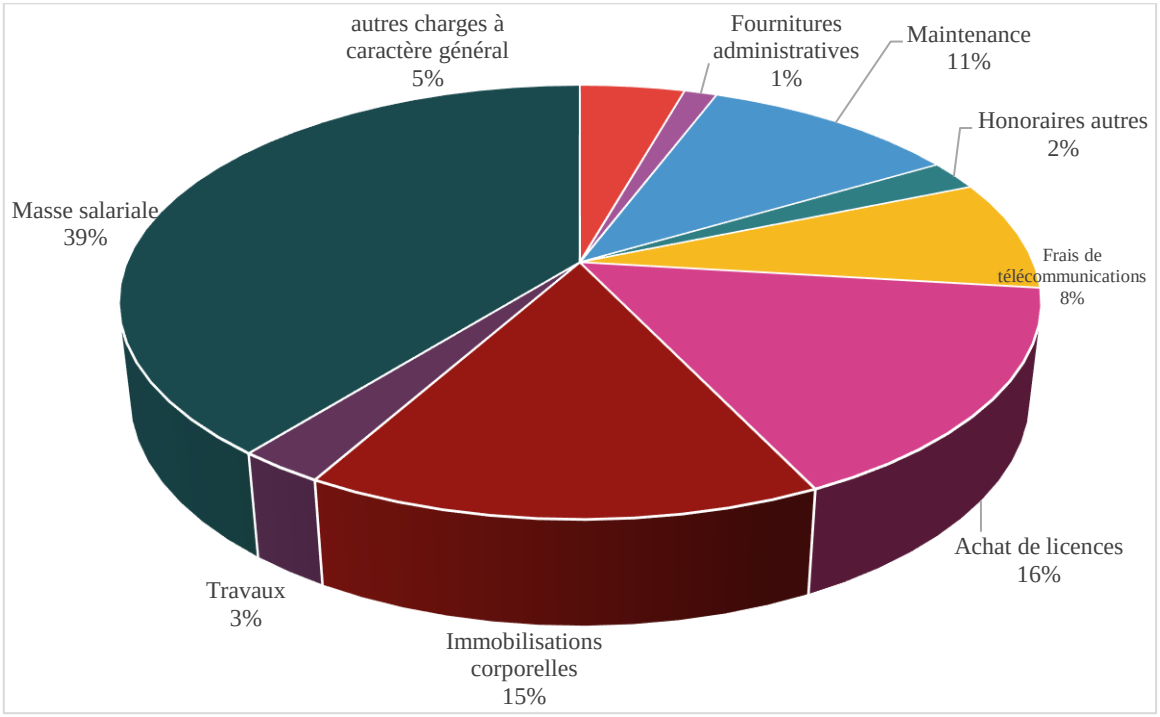
[14] Logiciels acquis près de l'union des groupements d'achats publics (UGAP) (+0,4 M€) et auprès de Nomios (0,1 M€).

Tableau n° 2 : Les dépenses de la DSN

En €	2016	2017	2018	2019	2020	2021	%
Charges à caractère général	2 206 045	2 126 335	2 091 169	2 275 380	2 187 469	2 373 473	1,5%
Fournitures administratives	130 752	143 359	155 408	102 833	73 382	65 711	-12,9%
Maintenance	1 029 110	973 425	921 239	951 235	801 163	627 991	-9,4%
Honoraires autres	155 102	149 174	128 749	289 259	182 115	178 242	2,8%
Frais de télécommunicat°	609 376	606 932	623 672	607 850	711 082	883 232	7,7%
Groupe d'élus (comm.)	345	309	94				-100,0%
Masse salariale	3 162 482	3 157 721	3 184 215	3 135 011	3 214 011	3 487 838	2,0%
Dépenses de Fonct.	**5 368 872**	**5 284 365**	**5 275 478**	**5 410 391**	**5 401 480**	**5 861 311**	**1,8%**
Charges de gestion CD	**535 935 731**	**535 094 646**	**520 714 268**	**525 705 945**	**538 703 384**	**541 098 283**	**0,19%**
% des charges de gestion	**1,00%**	**0,99%**	**1,01%**	**1,03%**	**1,00%**	**1,08%**	
Achat de licences	1 128 043	1 128 191	1 140 516	1 254 377	1 191 877	2 026 001	12,4%
Immobilisations corporelles	852 282	1 101 486	932 996	689 090	1 853 684	2 105 250	19,8%
Travaux	87 034	47 774	136 002	65 256	94 668	844 552	57,5%
Total général	**7 436 231**	**7 561 816**	**7 484 992**	**7 419 113**	**8 541 709**	**10 837 113**	7,8%

Source : CRC à partir des fichiers de mandats et des données du département pour la masse salariale.

Graphique n° 2 : Répartition des dépenses de la direction des services numériques



Source : CRC à partir des fichiers des mandats et des données du département pour la masse salariale.

4.3 La gestion des ressources humaines

4.3.1 Les effectifs

Les effectifs de la DSN du département du Morbihan sont globalement stables entre 2016 et 2020 et enregistrent une progression de 7,5 % en 2021 (+4,5 agents, portant les effectifs à 64,5 agents), concentrée sur les agents de catégorie A (+3,1 agents).

Tableau n° 3 : Répartition par catégorie des agents de la DSN du département du Morbihan

En ETP	2016	2017	2018	2019	2020	2021
Catégorie A	26	24	26	27	27	30,1
Catégorie B	23	23	23	20	23	23,2
Catégorie C	11	11	12	11	8	9,2
Non connu ou autres (apprentis)	2	2	1	2	2	2
Total	**62**	**60**	**62**	**60**	**60**	**64,5**

Source : Paies du département du Morbihan pour les mois de janvier de 2016 à 2020.

4.3.2 La couverture des compétences attendues

La structuration d'un service DSI s'articule autour de neuf métiers[15] : directeur des systèmes d'information, responsable production et support des systèmes d'information, responsable des études et applications des systèmes d'information, responsable sécurité des systèmes d'information, administrateur systèmes et bases de données, chef de projet technique des systèmes d'information, chef de projet études et développement des systèmes d'information, chargé de support et services des systèmes d'information et chargé des réseaux et télécommunications.

La DSN du département couvre l'ensemble des compétences attendues même si elle ne dispose pas de métiers spécifiques au traitement de la donnée ou en lien avec la cybercriminalité ou les risques de cyber-attaques. Même si le département ne dispose probablement pas de la surface pour justifier la présence à temps complet de ces métiers, cela peut constituer un frein aux activités du service à court terme.

[15] La description des métiers présents dans une DSI est disponible dans le répertoire des métiers du Centre national de la fonction publique territoriale (CNFPT), accessible sur son site internet.

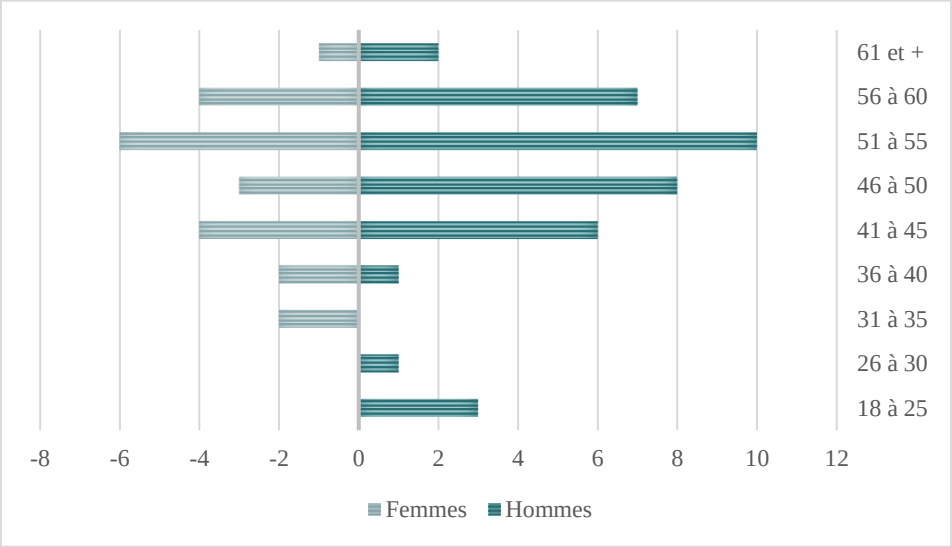
Des métiers en tension

Dans son panorama statistique des métiers territoriaux 2017-2019, le Centre national de la fonction publique territoriale (CNFPT) note que parmi les principaux métiers entrant en concurrence avec le secteur privé (1 576 citations), ceux de chef de projet technique des SI (45 citations), chargé de support et services des SI (30 citations) et administrateur systèmes et bases de données (21 citations), se situent respectivement aux 4e, 12e et 18e places des métiers les plus cités.

4.3.3 La formation des agents de la DSN

La pyramide des âges de la direction en 2020 donne à voir une moyenne d'âge de 48,4 ans et des agents de plus de 55 ans représentant 28 % des effectifs. Cela se traduit mécaniquement par des charges salariales importantes. Par ailleurs, dans un domaine caractérisé par des ruptures technologiques fréquentes, cette situation présente un risque nécessitant une politique de formation adaptée.

Graphique n° 3 : Pyramide des âges des agents de la DSN – janvier 2020



Source : CRC à partir des données de paie du département.

Entre 2019 et 2021, les agents de la direction n'ont suivi que 169,8 jours de formation (hors formations en alternance), soit 2,76 jours par ETP[16]. Parmi ces formations, la promotion du management et de la conduite de projets a représenté plus de 110 jours. Cette orientation illustre la volonté de confier à la DSN une place importante dans l'évolution des pratiques internes de la collectivité et de professionnaliser ses compétences pour répondre efficacement aux projets des différentes directions.

[16] À raison de 61,5 ETP par an en moyenne sur les exercices concernés.

La norme Cobit PO7 recommande de se doter d'un référentiel de compétences de la DSN ou d'une cartographie permettant d'évaluer les ressources internes et leur adéquation aux besoins actuels et futurs. Les décisions stratégiques concernant les ressources humaines doivent faire l'objet d'un plan actualisé périodiquement. Ce plan[17] doit lui-même se décliner en plans de recrutement, de formation, des évolutions individuelles et des achats externes de l'assistance complémentaire. La mesure de la mise en œuvre de ce processus passe par le suivi du plan de formation par rapport à la cartographie cible des compétences, le suivi du taux de réalisation des évaluations des collaborateurs ainsi que le taux de couverture des postes par une fiche de fonction.

Le département ne dispose pas de référentiel de compétences ni de parcours de formation pour les informaticiens de la DSN. La chambre recommande au département de doter la DSN d'un plan de formation spécifique, compatible avec une cartographie cible des compétences et **préconise l'organisation de formations en interne pour repérer des agents pouvant évoluer sur des métiers en tension comme la gestion de projet**.

En réponse aux observations provisoires de la chambre, le département a indiqué qu'un plan de formation spécifique à la DSN serait mis en place en lien avec la stratégie numérique.

Recommandation n° 4 Doter la DSN d'un plan de formation spécifique compatible avec une cartographie cible des compétences.

[17] La mesure de la mise en œuvre de ce processus passe par le suivi du plan de formation par rapport à la cartographie cible des compétences, par le suivi du taux de réalisation des évaluations des collaborateurs, ainsi que par le taux de couverture des postes par une fiche de fonction.

5 LA GESTION DES DONNEES

5.1 Le RGPD : un cadre réglementaire contraignant

Le règlement général sur la protection des données (RGPD) adopté en 2016 est entré en vigueur le 25 mai 2018[18]. Il encadre le traitement des données personnelles sur le territoire de l'Union européenne, dans un contexte d'évolution des technologies et des usages (recours accru au numérique, développement du commerce en ligne…). S'il s'inscrit dans la continuité de la loi française « informatique et libertés » de 1978, il renforce sensiblement le contrôle par les citoyens de l'utilisation qui peut être faite de leurs données.

Ce texte concerne tout organisme, quels qu'en soient la taille, le pays d'implantation et l'activité, publique ou privée, dès lors qu'il traite des données personnelles pour son compte ou non, s'il est établi sur le territoire de l'Union européenne ou si son activité cible directement des résidents européens. La notion de données personnelles est à comprendre au sens large puisqu'il s'agit de *« toute information se rapportant à une personne physique identifiée ou identifiable »*, que ce soit directement ou indirectement[19], à partir d'une seule donnée (numéro de sécurité sociale, ADN) ou à partir du croisement d'un ensemble de données.

Le traitement appliqué à ces données personnelles s'entend également au sens large : il s'agit d'une ou d'un ensemble d'opérations, portant sur ces données, quel que soit le procédé utilisé[20]. Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire qu'il n'est pas permis de collecter ou traiter des données personnelles dans la simple hypothèse d'un usage futur. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle de l'organisation.

Contrairement à la loi informatique et libertés de 1978, le RGPD ne soumet pas les traitements de données à caractère personnel à un régime d'autorisation préalable, mais il demande aux organisations, quelle que soit leur taille, de déployer un dispositif de responsabilisation des acteurs du traitement et fixe à leur égard une obligation de moyens et non de résultats. Chaque entité doit ainsi être en mesure de démontrer sa conformité aux principes et règles posés dans le règlement. Le RGPD fixe un certain nombre d'obligations concrètes de conformité, parmi lesquelles la nomination d'un délégué à la protection des données (DPD) et la tenue d'un registre de l'ensemble des traitements de données à caractère personnel réalisés dans cette entité, quelle qu'en soit la nature.

[18] Ses dispositions ont été transposées en droit français par la loi du 20 juin 2018 relative à la protection des données personnelles, son décret d'application du 1er août 2018, puis par l'ordonnance du 12 décembre 2018 et le décret du 29 mai 2019.

[19] Cette information peut être directe (nom, prénom) ou indirecte (identifiant, numéro de client, numéro de téléphone, donnée biométrique, éléments propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale), mais aussi voix ou image.

[20] Collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement.

Le RGPD donne aussi compétence aux autorités nationales (la Commission nationale de l'informatique et des libertés (Cnil) en France) pour contrôler a posteriori et, le cas échéant, sanctionner les entités qui méconnaîtraient les obligations fixées par le règlement. La Cnil, sur la base de signalements ou de plaintes, est ainsi habilitée, en fonction de sa propre analyse des risques, à effectuer des contrôles sur pièce et sur place dans un très large champ d'organismes. Les sanctions encourues en cas de non-conformité peuvent être particulièrement lourdes.

5.2 La conformité du département au RGPD

5.2.1 La politique de gestion des cookies

Le site internet du département demande l'acceptation de cookies. Si un lien vers la politique de confidentialité est proposé, ce dernier ne renvoie qu'aux mentions légales du site, avec un bref rappel sur les possibilités légales de s'opposer au traitement des données personnelles et au profilage. Par ailleurs, si le site donne l'adresse courriel du correspondant informatique et liberté, il ne mentionne pas les coordonnées du DPD. Par ailleurs, les finalités poursuivies par le traitement auquel les données sont destinées, la durée de conservation des données à caractère personnel ou, à défaut, les critères utilisés pour déterminer cette durée[21] ne sont pas plus renseignés.

La chambre recommande de rédiger et publier une véritable politique de confidentialité sur le site du département.

En réponse aux observations provisoires, le département a indiqué avoir mis en conformité les sites relevant de la culture et s'est engagé à lancer des travaux sur le site institutionnel au premier semestre 2023.

Recommandation n° 5 Adopter et mettre en ligne sur le site internet du département la politique de confidentialité des données recueillies.

5.2.2 La déléguée à la protection des données (DPD ou DPO)

Le délégué à la protection des données (DPD) est l'acteur principal chargé de la protection des données. Il doit informer et conseiller l'organisme en matière de protection des données, veiller au respect des principes et droits fixés par le RGPD dans les activités courantes, être le point de contact de la Cnil, notamment en cas de contrôle de l'organisme, être le point de contact de toute personne, extérieure à l'organisme, ou membre de celui-ci, qui souhaite exercer ses droits ou signaler une violation de ses données. Il doit également tenir à jour la documentation relative aux traitements réalisés par l'entité et enfin élaborer un bilan d'activité annuel.

[21] Mention imposée par l'article 104 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en vigueur depuis le 1er juin 2019.

Une DPD a été nommée le 1er janvier 2018, à temps plein. Membre du secrétariat général, elle est fonctionnellement rattachée au chef du service audit et appui aux politiques publiques et est mutualisée avec la MDA. Les rapports qu'elle produit sont de bonne qualité et traduisent une prise en compte réelle des obligations nées du RGPD. Celui de 2020 fait toutefois état d'une difficulté récurrente depuis sa désignation, tenant à ce que les informations à destination des directeurs et chefs de service sont insuffisamment relayées par les membres de la direction générale. Ce point mériterait d'être pris en compte par la collectivité.

5.2.3 L'état d'avancement de la mise en conformité au RGPD

Si la collectivité mène une politique active de mise en conformité avec le RGPD, celle-ci est loin d'être achevée. Sur les 202 processus qu'elle a identifiés, seulement 65 ont reçu un avis de la DPD. Si certains, parmi ceux traités, apparaissent particulièrement sensibles (gestion des offres d'emploi), plusieurs autres restent à compléter, à l'image des 70 processus de la DGISS, dont seulement 14 ont reçu un avis de la DPD. De même, sur 17 processus de la DSN, seulement deux ont reçu un avis, des processus particulièrement sensibles restant à traiter : accès wifi, contrôle individualisé des accès (renseigné dans le logiciel cependant), site web www.cg56.fr (collecte de CV, annuaires, demande d'information).

5.2.4 L'information de la Cnil et des gestionnaires de traitement

Le RGPD impose aux responsables de traitements de documenter, en interne, les violations de données personnelles et de notifier à la Cnil celles qui présentent un risque pour les droits et libertés des personnes. Une notification aux personnes concernées doit être effectuée lorsque le risque est élevé. Il revient à la Cnil et au DPD d'alerter les responsables de traitements des manquements à la conformité au RGPD.

Si ces obligations sont respectées dans le champ des processus ayant reçu un avis de la DPD, le département doit poursuivre son travail sur les autres processus.

5.3 Les contrats et le RGPD

Les contrats de la DSN et les cahiers des clauses administratives ou techniques particulières (CCAP/CCTP) comprennent des clauses compatibles avec le RGPD (capacité d'audit des fournisseurs, clauses concernant les données personnelles, etc.). Une note a été transmise en juillet 2019 à tous les services dont la DSI, les informant de l'obligation d'intégrer aux marchés publics les mentions informatiques et libertés. Une annexe spécifique sécurité et RGPD est annexée systématiquement à tous les marchés relatifs aux technologies de l'information et de la communication (TIC).

Plus globalement, un modèle de clauses RGPD est utilisé comme support de base pour les marchés et les contrats qui sont adaptés en fonction des prestataires. Les mesures qu'il comporte apparaissent satisfaisantes (demande de documentation, localisation des données, sous-traitants, etc.). Le service des achats fait preuve de vigilance sur ce point et constitue un relais important pour la DPD.

5.4 La politique d'ouverture des données (open data)

L'article L. 312-1-1 du code des relations entre le public et l'administration impose aux administrations et aux collectivités territoriales de plus de 3 500 habitants, de publier en ligne les bases de données, mises à jour de façon régulière, qu'elles produisent ou qu'elles reçoivent et qui ne font pas l'objet d'une diffusion publique par ailleurs, ou encore les données, mises à jour de façon régulière, dont la publication présente un intérêt économique, social, sanitaire ou environnemental. Il s'agit, par leur réutilisation, d'offrir de nouveaux services aux citoyens dans une logique de plateforme.

Le département n'a que peu investi cette politique d'ouverture des données. Il n'a ainsi mis en ligne sur data.gouv.fr que 20 jeux de données, parfois anciennes. À titre de comparaison, le département du Finistère publie 114 jeux de données sur sa plateforme « *Open Data* 29 ».

TABLE DES ANNEXES

Annexe n° 1. Glossaire

Agence nationale de la sécurité des systèmes d'information (ANSSI) : l'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV).

AMOA : l'assistant à maîtrise d'ouvrage est le prestataire chargé par le client (maître d'ouvrage ou MOA) de l'assister à différents stades d'un projet. C'est l'un des trois piliers qui interviennent dans la gestion des projets informatiques avec la maîtrise d'œuvre (MOE) et la MOA. C'est une fonction qui assiste la MOA dans l'atteinte de ses objectifs.

Antivirus : logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants.

Architecture informatique : cadre de référence intégré pour faire évoluer ou tenir à jour les technologies existantes et en acquérir de nouvelles afin d'atteindre les objectifs stratégiques et les objectifs métier.

Application : programme (ou un ensemble logiciel) directement utilisé pour réaliser une tâche, ou un ensemble de tâches élémentaires d'un même domaine ou formant un tout.

Attaque par hameçonnage (*phishing*) : attaque visant à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent.

Authentification / identification : procédure ayant pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

Base de données : permet de stocker et de retrouver des données structurées, semi-structurées ou des données brutes ou de l'information, souvent en rapport avec un thème ou une activité ; celles-ci peuvent être de natures différentes et plus ou moins reliées entre elles.

BitLocker : spécification de protection des données développée par Microsoft, qui fournit le chiffrement de partition.

Câble Ethernet : câble permettant de connecter un ordinateur à réseau.

Cartographie : outil essentiel à la maîtrise du SI, permettant d'avoir connaissance de l'ensemble de ses composants et d'obtenir une meilleure lisibilité de celui-ci en le présentant sous différentes vues.

Centre d'assistance (*helpdesk*) : service chargé de répondre aux demandes d'assistance émanant des utilisateurs de produits ou de services.

Chef de projet informatique : personne qui surveille le processus de développement logiciel, effectue la gestion de la configuration, identifie les problèmes de sécurité, de performance et de conformité, et prépare les exigences logicielles et les documents de spécification.

Cnil (commission nationale de l'informatique et des libertés) : créée par la loi « informatique et libertés » du 6 janvier 1978, elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Ainsi, elle veille à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle est une autorité administrative indépendante, c'est-à-dire un organisme public qui agit au nom de l'État, sans être placé sous l'autorité du gouvernement ou d'un ministre. Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction.

Cobit (*Control Objectives for Information and related Technology*, ou objectifs de contrôle de l'information et des technologies associées en français) : référentiel de bonnes pratiques d'audit informatique et de gouvernance des SI d'origine américaine. Au fil des versions successives, il tend à devenir un outil fédérateur de gouvernance des SI en intégrant progressivement les apports d'autres référentiels tels que ISO 9000, ITIL, etc.

Contrôle interne : politiques, procédures, pratiques et structures organisationnelles conçues pour fournir une assurance raisonnable que les objectifs métiers seront atteints et que les événements indésirables seront prévenus ou détectés et corrigés.

Cookies : petits fichiers stockés par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associés à un domaine web (c'est à dire dans la majorité des cas à l'ensemble des pages d'un même site web). Ces fichiers sont automatiquement renvoyés lors de contacts ultérieurs avec le même domaine.

Cybercriminalité : actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdéfense / cyberprotection : ensemble des mesures techniques et non techniques permettant à une organisation de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cybersécurité : état recherché pour un SI lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des SI et s'appuie sur la lutte contre la cybercriminalité et la mise en place d'une cyberdéfense.

Défaçage : résultat d'une activité malveillante visant à modifier l'apparence ou le contenu d'un serveur internet. Cette action malveillante est souvent porteuse d'un message politique et d'une revendication.

Déléguée à la protection des données (DPD) : personne chargée de la protection des données personnelles au sein d'une organisation. La fonction de DPD a été instaurée par les articles 37 et suivants du Règlement général sur la protection des données (RGPD). La désignation d'un DPD est obligatoire pour certaines entités privées, ainsi que pour l'ensemble des autorités publiques ou organismes publics (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle). La fonction peut être exercée par un salarié de l'entité ou par un DPD externalisé agissant sur la base d'un contrat de service.

Digitalisation : numérisation de documents afin de les sauvegarder sur un support informatique.

Faille de sécurité : faiblesse dans un SI permettant de porter atteinte à son intégrité, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Gouvernance : description des règles de direction et de contrôle d'un système. Elle associe le pilotage, c'est-à-dire s'assurer que les décisions actuelles préparent convenablement l'avenir, et le contrôle, c'est-à-dire mesurer l'écart par rapport à ce qui était prévu (Cigref).

ITIL (*Information Technology Infrastructure Library*, ou bibliothèque pour l'infrastructure des technologies de l'information) : ensemble d'ouvrages recensant les bonnes pratiques du management du SI. Rédigée à l'origine par des experts de l'Office public britannique du Commerce (OGC), ITIL a fait intervenir à partir de sa version 3 des experts issus de plusieurs entreprises de services telles qu'Accenture, Ernst & Young, Hewlett-Packard, Deloitte, BearingPoint, CGI ou PriceWaterhouseCoopers.

Logiciel : ensemble de séquences d'instructions interprétables par une machine et d'un jeu de données nécessaires à ces opérations. Le logiciel détermine donc les tâches qui peuvent être effectuées par la machine, ordonne son fonctionnement et lui procure ainsi son utilité fonctionnelle. Les séquences d'instructions appelées programmes ainsi que les données du logiciel sont ordinairement structurées en fichiers. La mise en œuvre des instructions du logiciel est appelée exécution et la machine chargée de cette mise en œuvre est appelée ordinateur ou calculateur.

Malware (ou logiciels malveillants) : terme générique utilisé pour désigner une variété de logiciels hostiles ou intrusifs : virus informatique, vers, cheval de Troie, *ransomware*, *spyware*, *adware*, *scareware*, etc. Il peut prendre la forme de code exécutable, de scripts, de contenus actifs ou d'autres logiciels, ce qui le différencie du phishing.

MOA (m**aître d'ouvrage)** : personne à l'origine du projet, entité juridique cliente, qui confie la réalisation du projet informatique à un ou plusieurs prestataires informatiques.

MOE (maître d'œuvre) : personne chargée de la réalisation de la solution informatique, objet du contrat conclu avec le client (MOA). Le MOE est garant de la bonne réalisation technique des solutions et fournit le produit. Il peut réaliser lui-même cette solution, ou missionner un ou plusieurs fournisseurs pour cette réalisation.

Numérisation : conversion des informations d'un support ou d'un signal électrique en données numériques, que des dispositifs informatiques ou d'électronique numérique pourront traiter. Les données numériques se définissent comme une suite de caractères et de nombres qui représentent des informations.

***Open data* ou données ouvertes** : données numériques dont l'accès et l'usage sont ouverts aux usagers, qui peuvent être d'origine privée mais surtout publique, produites notamment par une collectivité ou un établissement public.

Pare-feu (*firewall*) : outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

***Phishing*, ou hameçonnage** : forme d'escroquerie sur internet où le fraudeur se fait passer pour un organisme connu de l'utilisateur (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme afin de récupérer des coordonnées bancaires (numéro de compte, codes personnels, etc.).

Plan de Continuité d'Activité (PCA) : plan ayant pour but de garantir la survie de l'entreprise en cas de sinistre important touchant le SI. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entité.

Plan de reprise d'activité (PRA) : ensemble de procédures (techniques, organisationnelles, sécurité) permettant à une entreprise de prévoir par anticipation les mécanismes pour reconstruire et remettre en route un SI en cas de sinistre important ou d'incident critique. En cas de sinistre, le PRA permet de reconstruire les serveurs en leur affectant les données répliquées et ainsi de redémarrer les applications sous quelques minutes ou quelques heures, suivant les solutions retenues. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entité.

Politique générale de sécurité des SI (PGSSI) : plan d'actions définies pour maintenir un certain niveau de sécurité, reflétant la vision stratégique de la direction de l'entité (PME, PMI, industrie, administration, État, unions d'États…) en matière de sécurité des systèmes d'information (SSI).

Rançongiciels (*ransomware*) : technique d'attaque courante de la cybercriminalité, consistant en l'envoi d'un logiciel malveillant qui chiffre l'ensemble des données du destinataire et lui demande une rançon en échange du mot de passe de déchiffrement.

Règlement général sur la protection des données (RGPD) : texte de référence en matière de protection des données à caractère personnel.

Réseau informatique : ensemble d'équipements reliés entre eux pour échanger des informations.

Responsable Sécurité des SI (RSSI) : expert garantissant la sécurité du SI et assurant la disponibilité, l'intégrité et la confidentialité des données.

Risque : potentialité d'une menace donnée à exploiter les points faibles d'un actif ou d'un groupe d'actifs pour causer des pertes ou dommages à ces actifs ou à l'image de l'entité. Il se mesure en général par une combinaison de conséquences et de probabilités d'occurrences.

Sanctuarisation : dispositif cloisonnant physiquement à la fois la cage abritant les cœurs du SI, les chaînes applicatives critiques et les sauvegardes en les déconnectant des réseaux et des agents et en distinguant formellement les missions de l'administrateur de sauvegarde de celles de l'officier de sécurité chargé de la politique de sauvegarde à mettre en œuvre.

Sauvegarde : opération consistant à dupliquer et mettre en sécurité les données contenues dans un système informatique.

Système d'exploitation (*operating system*) : ensemble de programmes dirigeant l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.

Système d'information (SI) : ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs. Il s'agit d'un système socio-technique composé de deux sous-systèmes, l'un social et l'autre technique. Le sous-système social est composé de la structure organisationnelle et des personnes liées au SI. Le sous-système technique est composé des technologies (hardware, software et équipements de télécommunication) et des processus d'affaires concernés par le SI.

Tableau de bord : outil d'évaluation de l'organisation d'une entité, constitué de plusieurs indicateurs de sa performance à des moments donnés ou sur des périodes données.

Les publications de la chambre régionale des comptes Bretagne
sont disponibles sur le site :
https://www.ccomptes.fr/fr/crc-bretagne

Chambre régionale des comptes Bretagne
3, rue Robert d'Arbrissel
35042 RENNES CEDEX