Chambre régionale des comptes
Île-de-France

RAPPORT D'OBSERVATIONS DÉFINITIVES

LES SYSTÈMES D'INFORMATION DE LA RÉGION ÎLE-DE-FRANCE

Exercices 2016 et suivants

Observations
délibérées le 11 décembre 2020

TABLE DES MATIÈRES

SYNTHÈSE

La chambre régionale des comptes d'Ile-de-France a contrôlé la gestion des systèmes d'information de la région. La phase de l'instruction s'est prolongée d'avril 2019 à juin 2020. La phase de la contradiction sur la base du rapport d'observations provisoires a eu lieu d'août à novembre 2020.

La chambre a observé que, si les systèmes d'information de la région Île-de-France ont été en partie confortés depuis 2017, ils restent en deçà de la robustesse et de la sécurité nécessaires à une collectivité qui a fait du numérique un axe central de son action. Il en est particulièrement ainsi en ce qui concerne la gestion des données personnelles.

Le schéma directeur informatique de 2017 n'a été que partiellement mis en œuvre

L'adoption d'un premier schéma directeur informatique en juin 2017 a apporté un cadre pour l'arbitrage des décisions et la planification des projets. Le diagnostic initial, très critique, a conduit identifier 86 projets dont la mise en œuvre de 2017 à 2021 paraissait particulièrement ambitieuse.

À la suite de ce schéma, les postes de travail des services administratifs ont été mis à niveau à l'occasion de l'emménagement dans le nouveau siège de Saint-Ouen. De plus, de nouveaux outils numériques ont été déployés dans les 463 lycées publics. Des actions innovantes en direction des autres publics ont également été entreprises. Toutefois, plusieurs chantiers ont encore peu avancé : cartographie des infrastructures, sécurisation et formalisation de la politique de sécurité, élaboration d'un plan de secours, déploiement total du wifi dans les lycées.

L'organisation éclatée de la prise de décision ne permet pas une vision d'ensemble cohérente

L'organisation, avec trois pôles de décision distincts, paraît peu optimale. Certes, le fonctionnement des lycées, eu égard aux spécificités de leurs publics, peut justifier une gestion particulière des missions informatiques. Toutefois, on ne peut que s'étonner de la création d'une nouvelle direction chargée de la donnée et de la transformation numérique qui paraît renvoyer la direction des systèmes d'information (DSI) à des missions d'exécution alors que celle-ci est officiellement rattachée au directeur général.

Cette organisation favorise un émiettement de la prise de décision et une absence de vision d'ensemble consolidée à l'échelle de la collectivité.

En conséquence, certaines données de pilotage ne sont pas facilement disponibles comme l'état d'avancement du schéma directeur. Il en résulte aussi des coûts de coordination et de consolidation, qui ne sont pas évalués. Il est probable que ces défauts d'organisation ont nui à la capacité de la région à restituer l'état d'avancement de son schéma directeur.

Aussi, la chambre recommande à la région de mieux articuler la fonction informatique avec l'ensemble de ses missions et services pour en faire un outil de pilotage stratégique.

Grâce à un plan d'action adopté en 2018, les risques en matière de sécurité paraissent en voie d'être réduits

En matière de sécurité, la région n'objective pas ses priorités. Les démarches de cartographie des activités et des risques n'ont été que partiellement conduites malgré les rappels de la chambre dans ses précédents rapports. Faute d'identification au schéma directeur de 2017, la sécurité informatique a fait l'objet d'un plan d'action en 2018.

La région fait valoir qu'elle a lancé en septembre 2020 un vaste audit de sécurité sur l'ensemble de ses infrastructures informatiques, y compris des tests d'intrusion, dont les conclusions seront rendues en mai 2021. La chambre qui, n'a pu avoir accès aux résultats de cet audit, ne peut que prendre acte de cette démarche.

La région n'a pas pris toutes les mesures nécessaires pour s'assurer de la conformité au RGPD de la gestion des données personnelles

La région n'a pas été en mesure de démontrer à la chambre la conformité de sa gestion des données personnelles aux obligations réglementaires en la matière (RGPD : règlement pour la protection des données personnelles).

D'après les informations transmises au cours du contrôle, 289 traitements de données personnelles étaient labellisés activés dans l'outil de gestion dédié, pour un total d'environ 400 traitements inventoriés. De surcroît, cet inventaire est très partiel puisque neuf directions sur vingt 20, dont la direction générale mais aussi le cabinet de la présidente et le pôle de développement économique, n'avaient toujours pas estimé le nombre de traitements de données personnelles qu'elles exploitent.

En outre, la région n'a pas été en mesure de préciser lesquels de ces 289 traitements inventoriés (dont 25 sont classés comme sensibles) étaient conformes aux obligations du RGPD. Au cours du contrôle de la chambre, elle a expliqué que le taux de conformité des traitements n'était pas connu faute de données collectées et analysées pour établir cet indicateur. En réponse aux observations provisoires de la chambre, elle a ajouté que 356 traitements étaient déclarés dans son registre, ce qui n'a pu être vérifié.

Ainsi, la chambre observe que, plus de deux ans après la date limite de mise en œuvre du RGPD, la région reste dans l'incapacité de dénombrer ses traitements, d'en apprécier et d'en justifier la conformité.

Outre les risques qu'elle fait ainsi peser sur les personnes concernées par ces données, la région s'expose à des sanctions de la Commission nationale de l'informatique et des libertés (CNIL). La chambre lui recommande donc vivement de se mettre en conformité sans délai avec les règles applicables au traitement des données personnelles.

À la suite de ses observations, la chambre formule un rappel au droit et une recommandation de gestion.

RAPPEL AU DROIT ET RECOMMANDATION DU ROD

Au terme de ses travaux, la chambre adresse la recommandation et le rappel au droit repris dans la présente section.

La recommandation qui suit est un rappel au droit :

L'autre recommandations adressée par la chambre est la suivante :

« La société a le droit de demander compte à tout agent public de son administration »
Article 15 de la Déclaration des Droits de l'Homme et du Citoyen

1 PROCÉDURE

La chambre régionale des comptes d'Île-de-France a procédé au contrôle des comptes et à l'examen de la gestion des systèmes d'information de la région Île-de-France, pour les exercices 2016 et suivants.

Les différentes étapes de la procédure, notamment au titre de la contradiction avec l'ordonnateur, telles qu'elles ont été définies par le code des juridictions financières et précisées par le recueil des normes professionnelles des chambres régionales et territoriales des comptes, sont présentées en annexe n° 1.

La chambre a constaté que son instruction afin d'établir les observations provisoires a été marquée par la lenteur de réponse de la région, ainsi que par le manque d'exhaustivité des informations transmises. Certains compléments indispensables n'ont été transmis que lors de la réponse aux observations provisoires.

Ont participé au délibéré du présent rapport d'observations définitives, qui s'est tenu le 11 décembre 2020 sous la présidence de MM. Alain Stéphan, président de section, Romuald du Breil de Pontbriand, président de section, Philippe Grenier, premier conseiller.

Ont été entendus :

- M. Philippe Grenier, premier conseiller, assisté de Mme Valérie Carvajal, vérificatrice des juridictions financières, présentant le rapport de Mme Sandrine Taupin, première conseillère ;
- en ses conclusions, sans avoir pris part au délibéré, la procureure financière.

Mme Viviane Barbe, auxiliaire de greffe, assurait la préparation de la séance de délibéré et tenait les registres et dossiers.

La chambre a examiné la gouvernance, l'organisation et les coûts de la fonction informatique, la sécurité des systèmes d'information, ainsi que la conformité au règlement sur la protection des données personnelles.

Les conséquences de l'état d'urgence sanitaire à la fin du premier trimestre de 2020 n'ont pas été analysées dans le cadre du présent rapport.

2 LES SYSTÈMES D'INFORMATION : UN POINT DE FAIBLESSE HISTORIQUE DE LA COLLECTIVITE RÉGIONALE

L'instruction du présent contrôle a été conduite en référence aux notions et aux bonnes pratiques du secteur, qui sont notamment retracées dans le guide d'audit des systèmes d'information du Comité interministériel d'harmonisation de l'audit interne (CHAI), publiquement disponible, notamment sur le site des ministères économiques et financiers.

La région Île-de-France peut se référer à ce guide pour approfondir elle-même l'audit de ses systèmes d'information.

2.1 Les critères de bonne gestion d'un système d'information

Le système d'information (SI) représente l'ensemble des logiciels et matériels participant au stockage, à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation.

La fonction informatique vise à fournir à ces ressources l'organisation. Elle comprend donc, outre le système informatique, les personnes, processus, ressources financières et informationnelles qui y contribuent.

Un système informatique est constitué de ressources matérielles et logicielles organisées pour collecter, stocker, traiter et communiquer les informations. Les ressources humaines nécessaires à son fonctionnement (par exemple les administrateurs) sont parfois incluses dans ce périmètre.

Le système informatique ne doit pas être conçu comme une fin en soi : il est l'un des outils qui permet à l'organisation d'atteindre ses objectifs. Il ne se justifie qu'en tant qu'il soutient des processus « métier », sans lesquels il n'a aucun sens. Il doit donc être aligné avec les objectifs stratégiques de l'organisation. Cet alignement stratégique est fondamental : un système informatique est un facteur déterminant de la performance (efficacité, efficience, maîtrise des risques) d'une organisation. Inversement, un système informatique inadapté ou mal maîtrisé peut être une source inépuisable de difficultés.

Un SI idéal est donc à la fois en adéquation avec la stratégie de l'organisation et les objectifs des métiers, en conformité avec les obligations légales, sécurisé, facile à utiliser, fiable, adaptable, pérenne, disponible, efficient ; il respecte le plan d'urbanisme informatique et, lorsqu'il fait l'objet de marchés, ceux-ci sont conformes aux bonnes pratiques de la commande publique.

Les principaux facteurs clefs d'un système d'information performant sont les suivants :

- une forte implication de la direction dans la gestion du SI. Elle doit notamment superviser la gestion du SI par la mise en place des outils de pilotage suivants :
    - un schéma directeur informatique (SDI), qui définit la stratégie informatique pluriannuelle, dont la validation par la direction entérine l'adéquation entre la stratégie informatique et la stratégie de l'entité ;
    - des documents d'organisation de la gouvernance du SI, mis à jour régulièrement ;
    - des comités de pilotage informatiques réguliers (suivi des incidents, suivi des projets, suivi des budgets, etc.) au sein desquels la direction doit être représentée à bon niveau ;
    - des tableaux de bord de suivi de l'informatique ;
    - un portefeuille des projets SI et des analyses de la valeur des systèmes d'information ;
    - une politique de sécurité approuvée au plus haut niveau de la direction ;
    - des comités de sécurité réguliers au sein desquels la direction doit être représentée à bon niveau ;
    - une carte des applications et des systèmes informatiques à jour, incluse dans une politique d'urbanisme informatique.

- une politique de sécurité, validée et soutenue par la direction de l'organisme : la politique de sécurité des systèmes d'information (PSSI) est le principal document de référence en matière de sécurité des systèmes d'information (SSI). Elle reflète la vision stratégique de l'entité et montre l'importance qu'accorde la direction à la sécurité de son SI :
    - elle se matérialise par un document présentant, de manière ordonnée, les règles de sécurité à appliquer et à respecter dans l'organisme. Ces règles sont généralement issues d'une étude des risques SSI ;
    - après validation, la PSSI doit être diffusée à l'ensemble des acteurs du SI (utilisateurs, sous-traitants, prestataires). Elle constitue un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir ;
    - la PSSI est un document vivant qui doit évoluer afin de prendre en compte les changements de l'organisation, de missions et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux) ;
    - une charte d'utilisation du système d'information est souhaitable dans le but de sensibiliser les utilisateurs à la sécurité informatique et les informer des responsabilités qui leur incombent. Pour une meilleure efficacité, cette charte doit être signée par tous les agents et une communication régulière sur le sujet doit être mise en œuvre avec le support de la direction. Cette charte peut contenir par exemple les règles de sécurité et de bon usage (protection du PC, mots de passe, confidentialité, utilisation d'Internet, de la messagerie, protection du PC, etc.), les normes relatives aux logiciels (installation, licences, etc.), une description de la traçabilité des actions sur le SI à laquelle chaque utilisateur est assujetti et les sanctions applicables en cas de non-respect des règles décrites.
- le respect de la législation en matière de système d'information,
- le respect des bonnes pratiques en matière de commande publique,
- un paramétrage correct des droits d'accès aux applications informatiques,
- une bonne gestion des projets de développements informatiques.

Un SI est dit intégré quand toutes les applications communiquent entre elles de façon automatique à l'aide d'interfaces. Ainsi, les informations ne sont saisies qu'une seule fois dans les systèmes (notion de base de données maîtresse) et les échanges de données font l'objet de contrôles d'intégrité automatiques. L'action humaine, source potentielle d'erreurs ou de fraude, est donc très limitée.

2.2 Un manque de robustesse informatique signalé par la chambre de longue date

Les systèmes d'information de la région Ile-de-France ont été partiellement examinés dans trois précédents contrôles de la chambre portant sur le contrôle interne et la fiabilité des comptes (janvier 2009), la gouvernance de la collectivité (mai 2016) et la formation professionnelle continue (septembre 2018).

2.2.1 En 2009, une absence de stratégie informatique

En janvier 2009, à l'occasion de l'examen de la fiabilité du système financier et comptable, la chambre constatait la transformation du service informatique en direction à part entière (DSI) dans le cadre d'une réorganisation opérée en octobre 2005. Cette nouvelle direction était toutefois conçue comme un gestionnaire de moyens sans mission stratégique et sans participation aux instances de décision.

La chambre relevait que le système d'information n'était pas à la hauteur des enjeux de gestion de la première collectivité régionale française avec notamment :

- un manque d'urbanisation fonctionnelle : plus de 50 applications (hors outils bureautiques et logiciels métiers –voire « maison »), pas d'interfaces ni de système intégré de gestion ;
- une politique de sécurité non formalisée ;
- une charte d'utilisation des moyens informatiques non mise en œuvre.

Elle formulait quatre recommandations principales :

- considérer le système d'information comme un outil stratégique dans la conduite des missions de la collectivité régionale ;
- donner au service chargé du système d'information une place qui lui permette de participer activement aux décisions importantes ;
- créer un comité de direction ou de pilotage du système d'information sous l'égide du directeur général des services ;
- s'orienter vers un système intégré de gestion afin de partager l'information entre tous les acteurs et d'être en situation d'utiliser le système d'information comme outil d'aide à la décision.

2.2.2 En 2016, un début de démarche plus globale

Dans son rapport de mai 2016 sur la gouvernance de la collectivité régionale, la chambre constatait la mise en œuvre de ses recommandations avec notamment :

- un pilotage des systèmes d'information relevant du directeur général des services ;
- une gouvernance assez structurée ;
- une urbanisation en cours ;
- des actions récentes mais substantielles en matière de politique de sécurité (recrutement d'un responsable de la sécurité des systèmes d'information, mise en place d'un comité mensuel de sécurité).

La direction des systèmes d'information comptait alors 57 agents avec un budget de 10 M€ (hors lycées).

Dans ce rapport de mai 2016, la chambre constatait une démarche de pilotage, globale, prospective et suivie. À défaut de schéma directeur, les services informatiques s'inscrivaient dans une « feuille de route » réactualisée régulièrement depuis 2013, structurée autour de quatre objectifs stratégiques, déclinés en 22 objectifs opérationnels.

Elle relevait qu'une carte des risques avait été finalisée en 2014, portant sur les principaux risques internes (fraude et corruption, gestion des fonds européens, opérations financières, évolution des textes, contentieux, etc.).

La chambre appelait toutefois à une déclinaison en cartes opérationnelles, à l'instar de celle réalisée pour le champ de financement des tiers.

Aucune carte des risques informatiques n'avait été établie. De plus, certains risques étaient absents ou insuffisamment précisés dans le cadre général, comme les risques d'atteinte ou de rupture portant sur l'activité interne, les risques patrimoniaux, les risques portant sur l'image de la collectivité, le risque en matière de ressources humaines.

Les risques liés à une rupture de service informatique voire à une distorsion d'image n'avaient fait l'objet d'aucune analyse.

Des principaux constats de 2009 et 2016, il ressortait un écart significatif entre le niveau technique et organisationnel des systèmes d'information et la surface de la collectivité, que ce soit son budget, ses compétences, sa population ou son territoire.

Ainsi, la première direction des systèmes d'information a seulement été créée en 2005 et n'a été rattachée au directeur général des services qu'au début des années 2010. En 2015, l'urbanisation des systèmes d'information restait en cours et le premier responsable de la sécurité venait d'être recruté.

La chambre constatait toutefois que la collectivité ne s'était dotée ni d'un schéma directeur informatique ni d'une carte des risques informatiques.

2.2.3 En 2018, un besoin de cohérence et de fiabilité des données

Dans son rapport de septembre 2018, la chambre a pu observer les effets en matière de formation professionnelle continue de ce manque de structuration des outils informatiques. Aussi, a-t-elle recommandé de repenser ces outils, d'en fiabiliser les données et d'en contrôler la cohérence avec les paiements effectués.

Tableau n° 1 : Précédentes recommandations concernant les SI

L'action de la région en matière de formation professionnelle continue Contrôle n° 2017-0157
Recommandation n° 4 : Repenser les systèmes d'information dédiés à la formation professionnelle
Recommandation n° 5 : Fiabiliser les données pour bénéficier d'un instrument de pilotage de la politique de formation professionnelle
Recommandation n° 6 : Assurer un contrôle de la cohérence des systèmes d'information et de la régularité des paiements effectués

Source : rapport définitif (2018)

Interrogée sur les suites données à ces trois recommandations, la région a indiqué qu'un *« changement complet du système d'orientation »* a été décidé rapidement par le directeur général des services, et qu'une *« étude de faisabilité a été réalisée par un prestataire extérieur »*.

La région a précisé s'être orientée, mi 2019, vers une solution, déjà développée et utilisée dans les régions Auvergne Rhône Alpes, Nouvelle Aquitaine, Centre Val de Loire, limitant les développements « sur-mesure » et en conséquence, d'un coût maitrisé puisque partagé.

Elle a indiqué qu'en complément et en lien avec la nouvelle suite logicielle, elle a fait le choix d'acquérir un outil de pré-inscription (à destination des demandeurs d'emploi et des prescripteurs (Pôle Emploi et Missions locales). Cette brique logicielle permet de faciliter l'accès à l'offre de formation par l'usager ; elle permettra également à la région d'avoir une visibilité sur la demande et les taux de saturation des formations.

Le déploiement de ces solutions a, selon la région, démarré en juillet 2020 avec l'outil de positionnement qui devait être interfacé avec Pole Emploi au dernier trimestre 2020 et devrait se poursuivre pour un achèvement prévu à fin 2021.

En outre, la région a précisé en réponse aux observations provisoires de la chambre, que l'ancienne application restera en production dans les mêmes conditions, phase transitoire nécessaire au basculant dans le nouveau système.

3 UN SCHÉMA DIRECTEUR INFORMATIQUE INSUFFISAMMENT MIS EN ŒUVRE

3.1 De grandes ambitions régionales en matière d'innovation numérique

L'Île-de-France est la première région française au plan démographique et économique. La collectivité régionale est compétente pour :

- les transports, sous réserve de la compétence d'Île-de-France mobilité ;
- l'enseignement secondaire et le schéma régional de l'enseignement supérieur et de l'innovation ;
- la formation professionnelle et l'orientation ;
- le développement économique et l'innovation des entreprises ;
- le schéma régional d'aménagement, de développement durable et d'égalité du territoire ;
- le programme de développement rural et le plan régional de prévention et de gestion des déchets ;
- les fonds européens.

En outre, elle exerce des compétences partagées avec d'autres collectivités en ce qui concerne le sport, la culture, le tourisme, le logement, l'éducation populaire, la lutte contre la fracture numérique, la santé.

Le budget de la région est d'environ 5 Md€. Elle emploie plus de 10 300 agents : 8 500 dans les lycées et 1 800 dans les services du siège.

La majorité régionale élue en décembre 2015 a relancé les investissements à travers un plan de modernisation des infrastructures de transport, un engagement en faveur de l'enseignement supérieur et de la recherche, et la rénovation des lycées. Sur la période 2014-2019, les dépenses d'équipement ont ainsi progressé de près de 10 % par an en moyenne. Le bilan de mi-mandat a d'ailleurs souligné « la mise en mouvement des services régionaux », dont témoignerait un premier déménagement à Saint-Ouen (93), deux ans après l'installation du nouvel exécutif.

En matière d'informatique, les objectifs de l'exécutif sont à la fois de hisser la région au premier rang de la qualité de vie et réduire ses fractures territoriales et sociales[1], et d'en faire la première Smart région d'Europe, grâce à la transformation numérique du territoire[2].

Pour atteindre ces objectifs, la région ambitionne l'utilisation de dispositifs numériques innovants (intelligence artificielle, *big data*, Internet des objets) et de systèmes d'information performants, portés par une administration régionale en mesure de répondre aux attentes d'un nouveau genre des usagers et citoyens.

Le projet régional suppose donc des systèmes d'information robustes, à la fois comme outils d'une administration agile et comme vecteur central de services publics numériques.

[1] Bilan de mi-mandat #MA RÉGION BOUGE POUR MOI.
[2] Dossier de presse du programme Smart région Initiative du 21 novembre 2017.

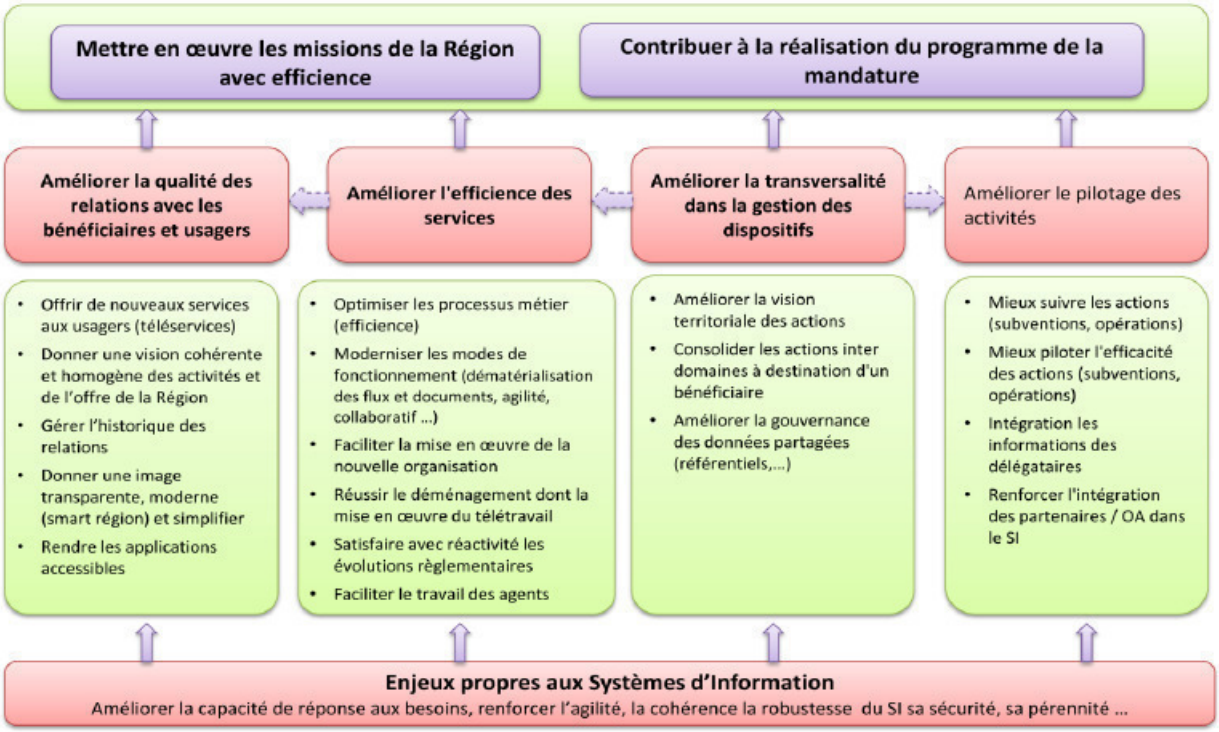
3.2 Un premier schéma directeur adopté en 2017 qui plaçait les systèmes d'information au cœur de la mandature

La région a adopté en juin 2017 un schéma directeur informatique très ambitieux, devant répondre à un diagnostic initial sévère, qui avait identifié de nombreux points à améliorer.

Selon les termes du document, son élaboration devait permettre d'aligner la stratégie en matière de système d'information sur les nouveaux enjeux de l'exécutif, élu fin 2015. Il s'agissait de disposer d'une feuille de route claire tant sur la ligne stratégique que sur sa déclinaison en termes de trajectoire et de moyens à mettre en œuvre.

Cette démarche reconnaissait donc aux systèmes d'information un rôle central dans l'exécution du programme de la mandature, tourné vers la modernisation des services à l'usager et la modernisation du fonctionnement interne de la collectivité.

Schéma n° 1 : Le schéma directeur 2017-2021



Source : schéma directeur, volet stratégique

Le diagnostic initial, établi au cours de l'année 2016, relevait notamment que le système d'information était incomplet, peu intégré et urbanisé avec une approche en silos très prononcée ; que des outils étaient obsolètes, mal paramétrés, mal utilisés, avec une dématérialisation trop peu avancée et des processus métiers trop peu formalisés et analysés.

Par ailleurs, le système d'information ne produisait pas d'informations de pilotage et son organisation n'offrait aucune garantie quant aux données publiées par la région (disponibilité, qualité et valeur).

Enfin, les systèmes comprenaient trop de progiciels, rendant l'architecture technique trop dépendante de chaque application.

L'élaboration de ce premier schéma directeur stratégique des systèmes d'information (SDSSI) 2017-2021 a donc répondu aux précédentes observations de la chambre.

La multiplication par quatre des projets retenus entre l'ancienne « feuille de route » informatique et le nouveau schéma directeur (de 22 à 86) témoigne à la fois d'un diagnostic sévère à l'égard de la situation antérieure et d'une volonté d'investir de champ des systèmes d'information.

Toutefois, son contenu foisonnant, qui couvre un large périmètre et recense de nombreux besoins (liés aux métiers et à la volonté d'accélérer la transformation numérique) interroge sur sa soutenabilité, dans un temps si contraint.

Trois actions majeures ont été réalisées depuis le 1er janvier 2016. Les deux premières, l'équipement informatique des services centraux et celui des lycées, s'inscrivent dans les objectifs de la mandature relatifs à la modernisation de son service public et de son fonctionnement. Ils ont été mis en œuvre en 2018 et 2019, illustrant le temps nécessaire à ce type de réalisations dont les prérequis techniques (performance et disponibilité des infrastructures et des réseaux) nécessitent eux-mêmes la conduite de plusieurs projets.

3.2.1 L'équipement informatique des agents de la région

Les avancées concernent tout d'abord les postes de travail individuels des agents de la région (outils permettant le télétravail mobile et connecté, la visioconférence, le partage d'écran et la téléphonie informatique).

S'y ajoutent les outils collectifs, déployés avec l'installation dans les nouveaux locaux (copieurs multifonctions, relais interne aux bâtiments dits *Influence 1 et 2* du signal téléphonique qui passe très mal à l'intérieur, déménagement du Data center).

Certaines améliorations ont ainsi été apportées en 2018 à la faveur de l'emménagement dans les nouveaux locaux et de la nouvelle conception du fonctionnement interne des postes de travail.

3.2.2 L'équipement informatique des lycées

Une mise à niveau de l'infrastructure informatique des lycées a été conduite pour préparer l'arrivée des équipements numériques (tablettes ou ordinateurs portables) permettant l'utilisation des nouveaux manuels scolaires dématérialisés, fournis par la région.

Ainsi, des dispositifs d'affichages collectifs en classe ont été installés et 177 000 équipements individuels ont été distribués aux élèves de 2nde et 1ère, dans les lycées volontaires, à partir de la rentrée scolaire 2019.

3.2.3 De nouveaux services en direction de la population

De plus, les projets regroupés sous le label *Smart Region* commencent à aboutir. La première version de la plateforme technique a été lancée le 15 octobre 2019. Elle propose quatre services : *Smart work*, (cartographie, recensement de tiers-lieux, fablabs, etc.) ; *Mon potentiel solaire* ; *IDF Data* (ouverture de données publiques et privées) ; *IDF 3D*, (description numérique du territoire et des projets d'aménagement).

D'autres services devaient être déployés en 2020 (données géographiques, aide à l'implantation d'entreprises, protection de l'environnement, réseaux de téléphonie mobile, informations partagées pour le secteur de la santé, suivi du contrat de plan État région).

3.3 Des faiblesses persistantes du fait d'un état d'avancement incomplet

Les réponses incomplètes de la région n'ont pas permis à la chambre de s'assurer de l'état d'avancement du schéma directeur dans son ensemble ni de chacun des projets qui y sont inscrits.

D'après les projets à venir en 2020, cités par la région au cours de l'instruction, des points de faiblesse majeurs restent encore à lever en matière de sécurité et d'infrastructures.

Il s'agit, pour les services en dehors des lycées :

- de la montée de version du système d'exploitation permettant le déploiement de Windows 10 et Office 365 sur tous les postes individuels ;
- des projets de sécurisation (protection antivirus des serveurs, protection des applications ouvertes sur l'extérieur, refonte des Proxy, gestion des mises à jour de sécurité, protection des postes de travail et chiffrement des disques durs, etc.) ;
- de la formalisation de la politique de sécurité ;
- de la création d'une carte des applications et des infrastructures et de la définition des règles d'urbanisme des systèmes d'information ;
- de la mise en place d'un plan de secours pour sécuriser le fonctionnement de la région, même en cas de perte d'une salle informatique.

Les projets en cours de déploiement dans les lycées relèvent des mêmes préoccupations :

- nouvelles architecture réseau (à poursuivre jusqu'en 2021) ;
- déploiement total du Wifi, au fur et à mesure de la mise à niveau du câblage et de l'architecture réseau ;
- remplacement ou mise à jour des serveurs (sécurité, anti-virus, mise à jour automatique des postes de travail) ;
- remplacement des contrôleurs de domaine obsolètes.

Ces projets correspondent au rattrapage de la dette technique qui pèse encore sur le fonctionnement interne des services. Ils constituent une étape indispensable pour envisager l'agilité escomptée.

Certes, en réponse aux observations provisoires de la chambre, la région a transmis un fichier de tableur relatif « à l'avancement des grands axes du schéma directeur des systèmes d'information ». Pour la chambre néanmoins, ce seul document ne constitue pas un réel outil de suivi du schéma directeur des systèmes d'information, dont il ne suit d'ailleurs pas l'architecture.

4 UNE GOUVERNANCE MULTIPLE ET INSTABLE

On désigne par gouvernance des technologies de l'information, la direction, les structures organisationnelles et les processus qui garantissent que les technologies de l'information soutiennent la stratégie et les objectifs de la collectivité territoriale[3].

[3] Institut Français d'Audit et du Contrôle internes (IFACI)

4.1 Une fonction informatique officiellement rattachée au DGS mais partagée entre plusieurs directions

D'après les déclarations effectuées par la région durant le contrôle, la fonction informatique est rattachée au directeur général des services (DGS) de la région. Force est de constater toutefois qu'elle est répartie entre trois directions, chacune en charge d'un volet du systèmes d'information :

- la direction des systèmes d'information,
- la direction de la donnée et du numérique au pôle achats, performance, commande publique, juridique,
- le service de la transformation numérique au pôle lycées.

Ainsi, la direction des systèmes d'information (DSI) n'est pas l'acteur unique ni même l'acteur central de la fonction informatique à la région.

Elle est principalement chargée du volet interne à destination des agents. Elle assure la conduite des projets techniques et bureautiques, la gestion du parc d'ordinateurs et de leur environnement, la définition et exploitation des infrastructures de communication et de télécommunication, le suivi du fonctionnement et de la maintenance des logiciels et progiciels en service.

Son organisation n'a que tardivement évolué. Seule une mission « fonctions transverses » a été créée en novembre 2017, dotée de quatre ingénieurs et chargée de la coordination de projets, de l'urbanisation, des outils et méthodes, ainsi que de la sécurité des systèmes d'information.

Outre la DSI, le pôle lycées gère de manière autonome, au moyen d'une équipe de 17 agents, les systèmes d'information et les matériels nécessaires à l'exercice de sa compétence.

Enfin, une direction de la donnée et du numérique, créée en septembre 2019 et rattachée au pôle achats, performance, commande publique, juridique, s'est vue confier les fonctions de pilotage stratégique. Elle regroupe des attributions qui était exercées depuis 2016 par les services de la direction générale.

La mission de cette direction renvoie la DSI aux seules missions de gestion des moyens informatique. Ainsi, le constat fait en janvier 2009 par la chambre a gardé en partie sa pertinence : une direction conçue comme un gestionnaire de moyens, sans mission stratégique à la hauteur des enjeux de gestion de la première collectivité régionale française.

Ces multiples évolutions de l'organigramme témoignent de la difficulté à concevoir la place des systèmes d'information dans l'administration régionale. Il résulte de cette organisation en triptyque un émiettement de la prise de décision et une absence de vision d'ensemble, consolidée à l'échelle de la collectivité, qui expliquent probablement les difficultés de la région à rendre compte de l'état d'avancement de son schéma directeur.

4.2 Les dispositifs de pilotage, prévus au schéma directeur de 2017, remplacés en 2019

Au cours du présent contrôle, la région n'a pas été en mesure de présenter clairement à la chambre son organisation en matière de conception et de mise en œuvre des décisions informatiques.

Dans une note du 29 août 2019, le directeur général des services a estimé qu'il était nécessaire d'identifier les projets stratégiques, d'une part, et de renforcer le pilotage, la vision transverse et la capacité de pilotage, d'autre part. Dans cette optique, la conduite des projets numériques a été confiée au directeur général adjoint chargé du pôle achats, performance, commande publique, juridique.

La région a donc pris acte que les comités de pilotage et de suivi, rattachés au directeur général en 2017, n'ont pas donné la satisfaction attendue, pour une mise en œuvre du schéma directeur informatique conforme aux objectifs initiaux.

Toutefois, n'ayant pas obtenu de la région les précisions demandées sur les méthodes d'arbitrage et de mises en cohérence, la chambre n'est pas en mesure de se prononcer sur l'amélioration que constituerait cette nouvelle gouvernance.

Elle ne peut que constater que le pilotage de la fonction informatique, initialement présenté comme une prérogative du directeur général, s'en trouve désormais fort éloigné. Les dispositions prises en 2017 n'auront donc pas vécu plus de deux ans.

4.3 Un budget informatique insuffisamment consolidé

En prévision comme en réalisation, la région n'a pas été en mesure de présenter à la chambre, en cours d'instruction, l'état annuel de ses dépenses informatiques et leur évolution depuis 2016.

Aucun document explicitant la procédure d'élaboration des prévisions budgétaires pour les besoins informatiques n'a été transmis à la chambre. Les montants correspondants pour les années 2016 à 2019 n'ont pas été fournis.

Il ressort d'une note sur la construction budgétaire, datée du 14 juin 2019, que la région a commencé à recenser les projets de modernisation informatique lors de l'élaboration du budget 2020. Rien n'était donc prévu dans ce domaine auparavant.

La région a fait valoir en réponse aux observations provisoires de la chambre que sa nomenclature budgétaire et comptable permettait d'identifier les dépenses informatiques au sein d'une annexe n° 1 Administration. Pour la chambre, connaître le coût associé à la mise en œuvre du schéma directeur reste néanmoins malaisé.

L'ensemble de ces observations conduit la chambre à constater que les modalités de gouvernance (une fonction informatique divisée entre trois directions, un pilotage éloigné de la direction générale) n'ont pas fait la preuve de leur efficience pour la mise en œuvre du schéma directeur informatique ou pour la gestion des moyens financiers nécessaires.

Il paraît vraisemblable que ce défaut d'organisation a contribué à ralentir la capacité de la région à répondre aux interrogations de la chambre au cours du présent contrôle.

La présidente du conseil régional a répondu aux observations provisoires de la chambre qu'elle allait entamer une réflexion pour améliorer encore le pilotage de ses systèmes d'information.

Recommandation n° 1 : Mieux articuler la fonction informatique avec l'ensemble des missions de la région en vue d'en faire un outil stratégique.

5 DES ACTIONS RÉCENTES POUR AMÉLIORER LA SÉCURITÉ INFORMATIQUE

5.1 La sécurité informatique et le schéma directeur 2017-2021

La sécurité des systèmes d'information n'a pas été relevée comme un point à améliorer dans le diagnostic initial de 2016. Elle n'apparaît dans schéma directeur ni comme un axe stratégique ni comme une action faisant l'objet d'une fiche projet.

La sécurité entre, parmi d'autres sujets, dans les « enjeux propres aux systèmes d'information (améliorer la capacité à répondre aux besoins SI Métiers, renforcer la cohérence du SI, sa sécurité, sa pérennité) ».

On ne peut que s'étonner de cet oubli, tandis que la chambre avait souligné les carences en la matière, dans son rapport de 2009, et qu'elle saluait les premières mesures prises, dans son rapport de 2016, avec la nomination d'un responsable de la sécurité et la mise en place d'un comité de suivi.

En réponse à ces observations, la région a précisé que la sécurité figure dans les enjeux à satisfaire du schéma directeur, mais qu'elle n'était pas un point de défaillance en 2016, et qu'aucune attaque contre ses systèmes d'information SI n'a abouti. Elle souligne en revanche que le diagnostic réalisé en 2018-2019 a identifié des points d'amélioration qui ont déclenché un chantier de mise à jour des infrastructures.

Il est heureux que la région n'ait eu à subir aucune attaque informatique réussie. La chambre constate que les chantiers entrepris récemment vont dans le sens d'une amélioration de la sécurité des systèmes d'information régionaux.

5.2 Des risques informatiques mieux pris en compte

Depuis les constats de 2009, la région n'a pas s'est pas dotée d'une politique de sécurité et n'a pas établi une carte de ses risques informatiques.

Elle a précisé, en réponse aux observations provisoires de la chambre, que la cartographie des risques et la politique de sécurité étaient en cours de rédaction, avec une échéance prévue en 2021.

La fonction de responsable des systèmes d'information, identifiée en 2015, a perduré. Rattachée à la direction des systèmes d'information, elle ne couvre pas l'ensemble du champ informatique. En effet, la région estime que la sécurité des systèmes d'information relatifs aux lycées et aux services numériques relève d'organismes et d'acteurs extérieurs : les responsables de sécurité des systèmes d'information académiques et la société prestataire de la smart plateforme.

De son côté, la direction des systèmes d'information a établi un plan d'action de sécurité informatique, en juin 2018, à partir de sa cartographie applicative, sa cartographie du réseau, de la réalisation de deux tests intrusion (pour deux applications hébergées chez un prestataire externe), et son auto-diagnostic.

Étalé sur trois ans, le plan est articulé autour de 15 axes et 57 projets, déclinés par ordre de priorité et par critère de complexité. Un tiers des projets (28 sur 57) sont classés comme « à initier au plus tôt » (priorité 1 – forte). Aucun chiffrage précis des dépenses correspondantes n'a été produit.

De plus, aucun plan de reprise informatique n'a été formalisé. Destiné à garantir la continuité de l'activité, celui-ci doit normalement définir les processus de restauration et de mise en production des données, à la suite d'un incident majeur. La région, en réponse aux observations provisoires de la chambre, estime que les infrastructures mises en œuvre depuis 2017 permettent une reprise d'activité en cas de perte d'une des deux salles informatiques et que la continuité de nombreuses applications métiers est assurée par leur externalisation.

Outre les deux tests d'intrusion déjà cités, aucun audit de sécurité n'a été réalisé. Au cours de l'instruction les pôles lycées et achats ont annoncé des actions dans ce domaine en 2020.

En réponse aux observations provisoires de la chambre, la région a précisé qu'un audit de sécurité avait commencé en septembre 2020, avec une échéance en mai 2021. L'élaboration du plan de continuité devrait lui succéder.

5.3 Une sensibilisation récente des agents à la sécurité informatique

La sensibilisation des agents à la sécurité informatique consiste à envoyer des messages électroniques de façon ciblée en fonction des attaques informatiques subies. Sans être inutile, cette seule action paraît insuffisante au regard des risques encourus par toute organisation fortement informatisée.

En réponse aux observations provisoires, la région a précisé que la charte informatique était disponible sur son intranet et qu'elle était donc facilement accessible à tous les agents. La chambre maintient qu'une communication spécifique sur l'existence de cette charte et de ses conseils en matières de sécurité complèterait utilement les envois de messages électroniques déjà évoqués.

Selon les dernières informations fournies à la chambre, un marché de « sensibilisation à la sécurité des SI » avec un budget prévisionnel de 100 000 € devait être lancé fin 2020.

En conclusion, la chambre relève que le sujet sensible de la sécurité informatique, qui a souffert d'un manque d'intérêt de la part de la collectivité, a été repris en main récemment.

6 UNE PROTECTION DES DONNÉES PERSONNELLES INSUFFISAMMENT GARANTIE

6.1 Un cadre réglementaire ancien avec de nouvelles obligations depuis mai 2018

Le cadre juridique applicable à la protection des données personnelles a été posé en France par la loi dite « informatique et libertés » de 1978[4], qui définit pour la première fois les règles et principes à respecter lors d'un traitement de données à caractère personnel. Elle précise également les compétences et missions de la Commission nationale de l'informatique et des libertés (CNIL), pour en assurer le respect.

Un nouveau règlement général sur la protection des données (RGPD)[5] a été adopté en 2016. Entré en vigueur le 25 mai 2018, il vise à donner aux citoyens européens davantage de visibilité et de contrôle sur leurs données personnelles. Ses dispositions ont été transposées en France par la loi du 20 juin 2018 relative à la protection des données personnelles[6], son

[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[5] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[6] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

décret d'application du 1er août 2018, l'ordonnance du 12 décembre 2018 et le décret du 29 mai 2019.

Le champ d'application du RGPD est particulièrement étendu : il s'impose à toute organisation publique ou privée, établie sur le territoire de l'Union européenne ou qui, pour son compte ou celui d'un tiers, traite des données personnelles appartenant à des citoyens de l'Union.

Contrairement à l'esprit de 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 : il met en place 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 donne aussi compétence aux autorités nationales (en France, la CNIL) pour contrôler a posteriori et, éventuellement, pour 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.

Dans ce nouveau cadre réglementaire[7], la donnée personnelle se définit comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Sont ainsi des données à caractère personnel toutes les informations, manuscrites ou numériques, qui permettent d'identifier directement ou indirectement une personne. Il en va ainsi par exemple, d'un relevé d'identité bancaire, d'un CV, d'une adresse, d'une plaque d'immatriculation, d'une adresse IP, d'une photographie d'identité, etc.

Les données appartiennent à trois types.

- type 1 : données non sensibles n'ayant pas un impact fort sur les droits et libertés de personnes (État civil, courriel, téléphone, etc.),
- type 2 : données non sensibles ayant un impact fort sur les droits et libertés des personnes (composition familiale, coordonnées bancaires, signature, diplôme, etc.),
- type 3 : données sensibles au sens de l'article 9 et 10 du RGPD (opinions politiques, syndicales, croyances religieuses, prétendue appartenance ethnique ou raciale, condamnations pénales, etc.).

On parle de traitement lorsque ces données font l'objet d'une opération, quel que soit le procédé utilisé, automatisé ou non[8]. Ainsi, un dossier papier de recrutement contenant des CV est un traitement de données à caractère personnel, de même qu'un dispositif de vidéosurveillance, un logiciel de paie, un fichier tableur contenant des adresses e-mail, une base de données, etc.

Les données et les traitements de données personnelles ainsi définis relèvent d'un responsable de traitement : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Toutefois, une attention particulière doit être portée à la notion de « sous-traitant », laquelle renvoie à « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du

[7] Article 4 Définitions.
[8] « Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

traitement ». Il ne s'agit donc pas ici du périmètre usuel de sous-traitance comme on peut le concevoir en matière de commande publique. Il englobe tous les opérateurs (les lycées par exemple) avec lesquels une politique régionale est conduite, dès lors que des données traitées sont en cause, quelle que soit la nature des relations juridiques.

6.2 Les principales obligations à respecter

La protection garantie par le RGPD repose sur cinq principes fondamentaux, qui doivent guider toutes les opérations de traitement de données à caractère personnel :

- le principe de licéité : le traitement doit avoir un fondement juridique (le consentement de la personne, l'exécution d'un contrat, le respect d'une obligation légale, la sauvegarde d'intérêts vitaux, l'exécution d'une mission d'intérêt public ou la poursuite d'intérêts légitimes par le responsable de traitement, etc.) ;
- le principe de loyauté : les personnes dont les données sont traitées doivent en être informées de façon claire, lisible et compréhensible. Elles doivent connaître notamment le périmètre du traitement, la base juridique qui l'autorise, la durée de conservation des données et les coordonnées des personnes auprès de qui faire valoir leurs droits ;
- le principe de finalité : les données traitées le sont pour une finalité déterminée, explicite et légitime. Une fois collectées, elles ne peuvent donc pas être utilisées pour satisfaire une autre finalité ;
- le principe de minimisation : au regard de leur finalité, les données traitées sont adéquates, pertinentes, limitées au strict nécessaire, exactes et tenues à jour ;
- le principe de limitation de la durée de conservation : sauf rares exceptions – notamment la conduite de recherches scientifiques ou historiques – les données traitées ne sont conservées que pendant la durée nécessaire à la poursuite de la finalité pour laquelle elles ont été collectées.

De plus, les entités doivent procéder à la nomination d'un ou d'une déléguée à la protection des données (DPD ou DPO, pour *data protection officer)*, et organiser la tenue d'un registre de l'ensemble des traitements de données à caractère personnel, quelle qu'en soit la nature.

Le RGPD crée également certaines obligations vis-à-vis des personnes dont les données sont traitées. Sans être exhaustif, on peut citer trois exemples.

- l'obligation de donner suite dans un délai d'un mois à toute demande d'exercice de leurs droits par les personnes dont les données font l'objet d'un traitement. Cela inclut notamment – sauf rares dispositions contraires – de leur donner le droit d'accéder à leurs données, de leur donner toute information qu'elles requièrent sur l'existence et le périmètre d'un traitement les concernant, de leur permettre de rectifier les données qui ont été traitées ou de les faire effacer, ou encore de leur permettre de demander la limitation ou de s'opposer au traitement réalisé ;
- l'obligation de documenter toute violation de données à caractère personnel, qu'elle soit accidentelle ou illicite, dès lors qu'elle entraîne la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé aux données qui ont été collectées. En cas de risque pour les droits et libertés des personnes concernées, la notification de la violation doit être faite sans délai à la CNIL et, en cas de risque élevé, les personnes concernées doivent être directement informées par l'organisme ;
- l'obligation de réaliser des études d'impact (ou PIA pour *privacy impact assessment*) lorsque des projets susceptibles d'exposer à un risque élevé la protection de la vie privée de tiers sont envisagés dans l'entité.

Ainsi, l'entrée en vigueur du nouveau règlement général pour la protection des données suppose des mesures d'adaptation significatives, à prendre par chaque organisme, pour assurer sa mise en conformité.

Pour maîtriser les risques à l'échelle d'un organisme, il paraît indispensable de diffuser une « culture » de la protection des données personnelles, notamment par des actions de sensibilisation, en particulier auprès du personnel et des directions les plus exposés (direction des systèmes d'information, direction des ressources humaines, etc.).

Des mesures organisationnelles fondées sur une analyse détaillée des risques doivent être prises pour protéger les données, en particulier les plus sensibles (données de santé, données bancaires, données de paie).

Des clauses spécifiques doivent être introduites dans les contrats et marchés pour tenir compte des obligations incombant aux différentes parties au titre du RGPD.

6.3 Une mise en conformité partielle et tardive au sein de la région Île-de-France

Le contrôle de la chambre a été conduit en référence à la démarche en six étapes obligatoires, préconisée par la CNIL : désigner un délégué à la protection des données, cartographier les traitements de données personnelles, prioriser les actions à mener sur la base de cette cartographie, gérer les risques identifiés le cas échéant via une analyse d'impact, organiser les processus internes, documenter la conformité.

6.3.1 La nomination d'un délégué à la protection des données et l'organisation de la documentation conformes à la réglementation

Le délégué à la protection des données a été désigné et déclaré auprès de la CNIL. Cette personne exerçait précédemment la fonction de correspondant informatique et liberté (CIL), créée à la région en 2009, dans le cadre de la loi de 1978. Cette continuité a permis de satisfaire aux obligations de nomination d'un délégué à la protection des données dans les délais réglementaires.

Le délégué est assisté par un réseau constitué à partir des anciens relais informatiques et liberté, réseau qui couvrait et couvre toujours l'ensemble des directions. Les supports des formations assurées par le délégué à ces correspondants témoignent d'une action de mise à niveau réglementaire et de diffusion des procédures adoptées par la région.

Toutefois, le rattachement du DPD au pôle achats, performance, commande publique, juridique, sans même apparaître dans l'organigramme, interroge sur la ligne hiérarchique entre cet agent et le directeur général, qu'il est censé informer et conseiller, selon les termes de sa lettre de mission.

Par ailleurs, la continuité entre CIL et DPD a permis de s'appuyer sur l'existant pour documenter la conformité : la région a fourni les éléments pour toute la période contrôlée, y compris les années 2016 (charte informatique) et 2017 (bilan d'activité du correspondant informatique et liberté), antérieures au RGPD.

Les fiches de procédure qui permettent de tenir à jour la documentation de la conformité ont été produites.

L'obligation de documentation, telle qu'elle est nouvellement définie, a bien été satisfaite dans les délais attendus.

6.3.2 Des choix de pilotage insuffisants pour garantir le respect des échéances et la protection des données personnelles

Le directeur général des services a été saisi par note du directeur général adjoint du pôle achats, performance, commande publique, juridique, le 29 août 2017, pour la mise en œuvre du RGPD à la région, soit neuf mois avant l'échéance.

Une équipe projet a été constituée sur la base des anciens relais informatiques et libertés (devenus correspondants DPD). Les sept comptes rendus transmis couvrent la période allant du 14 décembre 2017 au 24 mai 2019 (date de dernière modification du document). Ils permettent de constater que le comité de projet s'est saisi activement de sa mission. Ils témoignent également du faible niveau d'implication de la direction générale, bien des actions devant se traduire par « une note au DG ».

Toutefois, la mise en place de ce comité opérationnel, cinq mois avant l'échéance, était trop tardive pour espérer assurer la mise en conformité d'un organisme aussi étendu que la région à la date prescrite (25 mai 2018). Dans ce domaine, la région a manqué de célérité dans l'adaptation à un nouveau cadre réglementaire. De fait, deux ans après l'échéance, elle n'était pas en mesure de garantir la protection des données personnelles qu'elle utilise.

D'après les dernières informations transmises à la chambre, 289 traitements seraient publiés au registre (labellisés *activés* dans l'outil de gestion dédié), pour un nombre de traitements estimés à environ 400. Encore ne s'agit-il que d'un inventaire partiel, seulement 55 % des pôles ou directions ayant réalisé l'inventaire de leurs traitements. A la date du 17 juillet 2020, 9 directions sur 20 n'avaient toujours pas estimé le nombre de traitements de données personnelles qu'elle réalise (dont la direction générale, le cabinet, le pôle développement économique).

Tableau n° 2 : Inventaire des traitements de données personnelles au 17 juillet 2020

		Traitements inventoriés				Nombre estimé
	Inventaire	Type1	Type2	Type 3	Total	
DGS	NON	0	0	0	0	A fournir
SG	OUI	11	2	4	17	17
Cabinet	NON	0	0	0	0	A fournir
Plycées	OUI	5	2	0	7	7
PDEEF	En cours	0	0	0	0	A fournir
PCT	OUI	33	0	0	33	33
POLOT	OUI	0	0	1	4	4
TRESOR	OUI	32	20	3	55	55
PMS3/DICOMAP	OUI	3	0	0	3	3
PMS3/SOL	NON	0	0	0	0	A fournir
PAECIT	NON	0	0	0	0	A fournir
PFIN	OUI	7	12	0	19	19
PAPCPJ	OUI	4	4	6	14	14
DSI	En cours	0	0	0	0	A fournir
Culture	OUI	84	12	5	101	101
COM	En cours	0	0	0	0	A fournir
PRH	OUI	45	73	22	140	140
Médiateur	OUI	0	0	1	1	1
CESER	En cours	0	0	0	0	A fournir
PPMG	En cours	0	0	0	0	A fournir
Totaux		224	125	42	394	394

Source : région Île-de-France

Outre que la région ignore toujours le nombre de traitements de données personnelles qu'elle utilise, elle n'est pas en mesure d'en garantir la conformité, y compris pour les données les plus sensibles. Elle a expliqué en effet que « pour l'instant, le taux de conformité des traitements n'est pas connu, faute de données collectées et traitées spécifiquement pour renseigner cet indicateur ».

Ainsi, les 289 traitements (dont 25 environ de type 3) publiés au registre de la région sont possiblement conformes – ou non conformes – aux obligations réglementaires en matière de protection des données personnelles.

La région a précisé en réponse aux observations provisoires de la chambre que 356 traitements[9] sont déclarés dans son registre, ce qui n'a pu être vérifié.

La chambre constate que la manière dont la région a organisé la prise en compte du changement réglementaire ne lui a permis ni de respecter ses nouvelles obligations ni de garantir la protection des données personnelles qu'elle détient.

Plus de deux ans après la date limite de mise en œuvre du règlement pour la protection des données personnelles, la région reste dans l'incapacité de dénombrer ses traitements et d'en apprécier la conformité.

Elle a répondu à ces observations qu'elle avait fait le choix de passer par un prestataire extérieur pour assurer l'ensemble de ses obligations dans les meilleurs délais. Toutefois, la chambre rappelle que cette décision d'externalisation ne saurait l'exonérer de sa responsabilité d'une mise en conformité immédiate.

Rappel au droit n° 1 : Finaliser sans délai la mise en conformité réglementaire des traitements de données personnelles.

[9] La région dans sa réponse aux observations provisoires fait état par ailleurs, d'un autre chiffre -394 traitements-, sans donner d'indications sur la différence entre ces deux données.

ANNEXE UNIQUE : déroulement de la procédure

Le tableau ci-dessous retrace les différentes étapes de la procédure définie par le code des juridictions financières aux articles L. 243-1 à L. 243-6, R. 243-1 à R. 243-21 et par le recueil des normes professionnelles des chambres régionales et territoriales des comptes :

Objet	Dates	Destinataire
Envoi de la lettre d'ouverture de contrôle	8 avril 2019 reçue le 9 avril 2019	Mme Valérie PÉCRESSE, présidente
Entretien de début de contrôle	15 mai 2019	Mme Valérie PÉCRESSE, représentée par M. David BONNEAU, DGS, en présence de M. Paul BÉRARD, DGA du pôle finances, M. François SUBRENAT, Directeur des systèmes d'information, Mme Alexa GUÉNA-ANDERSSON, Directrice de la comptabilité
Entretien de fin d'instruction	18 juin 2020	Mme Valérie PÉCRESSE, représentée par M. David BONNEAU, DGS, en présence de Mme Sylvie VIDAL, adjointe au DGA du pôle finances et directrice du budget, M. François SUBRENAT, Directeur des systèmes d'information
Délibéré de la formation compétente	4 août 2020	
Envoi du rapport d'observations provisoires	21 août 2020	Mme Valérie PÉCRESSE
Envoi d'extraits du rapport d'observations provisoires	-	
Réception des réponses au rapport d'observations provisoires et aux extraits	2 novembre 2020	M David BONNEAU DGS, dûment mandaté par Mme Valérie PECRESSE
Auditions	-	
Délibéré de la formation compétente	11 décembre 2020	
Envoi du rapport d'observations définitives	18 décembre 2020	Mme Valérie PÉCRESSE
Réception des réponses au rapport d'observations définitives	12 février 2021	

Conformément aux articles L. 243-4 et L. 243-5 du code des juridictions financières, la Région Ile-de-France a disposé du délai d'un mois pour communiquer sa réponse écrite au rapport d'observations définitives que lui a adressée la chambre régionale des comptes d'Ile-de-France le 18 décembre 2020.

Aux termes du code précité, la lettre reçue par la chambre, datée du 12 février 2021 et hors délai, ne peut être considérée comme la réponse de la collectivité. Comme déjà rappelé, l'article R. 243-13 précise que le destinataire du rapport d'observations définitives peut adresser à la chambre une réponse « qu'il signe personnellement ».

« La société a le droit de demander compte
à tout agent public de son administration »
Article 15 de la Déclaration des Droits de l'Homme et du Citoyen

Chambre régionale des comptes Île-de-France
6, Cours des Roches
BP 187 NOISIEL
77315 MARNE-LA-VALLÉE CEDEX 2
Tél. : 01 64 80 88 88
www.ccomptes.fr/fr/crc-ile-de-france