

Rapport d'activité du Commissaire à la protection des données

juin 2024 – mai 2025

Table des Matières

Avant-propos

1. Introduction
2. Présence physique au siège de l'Organisation et représentation
 - 2.1 *Visites au Conseil de l'Europe*
 - 2.2 *Participation à des événements extérieurs*
3. Conseils et recommandations aux entités du Conseil de l'Europe
 - 4.1 *Direction des Services Généraux*
 - 4.2 *Direction des Ressources Humaines*
 - 4.3 *Direction des Technologies de l'Information (DIT)*
4. Déléguée à la protection des données
5. Statuts et Organisation du Commissaire à la protection des données
6. Conclusions

Avant propos

Le 28 janvier 1981, la Convention 108 était ouverte à la signature des Etats membres du Conseil de l'Europe et entré en vigueur en 1985. En 2011, débutait les travaux de modernisation du seul traité international juridiquement contraignant dans le domaine de la protection des données et ratifié par l'ensemble des membres du Conseil de l'Europe et 9 Etats tiers. Ces travaux ont débouché sur un protocole d'amendement adopté par le comité des Ministres le 18 mai 2018 et ouverts à la signature des Parties le 10 octobre de la même année. Le protocole entrera en vigueur lorsqu'au moins 38 parties l'auront ratifié. A ce jour 33 ratifications ont été déposées. Or il devient des plus urgents que le seuil minimum des 38 ratifications soit atteint rapidement pour l'avenir du droit à la protection des données en Europe et dans le monde. Dans le cas contraire, cette Convention pourrait devenir désuète et l'intérêt qui lui est porté bien au-delà du continent européen diminué fortement, portant ainsi atteinte à la crédibilité du Conseil de l'Europe. Or qu'il soit rappelé ici que ce texte conventionnel constitue le pilier et le pivot d'une réglementation universelle en matière de protection des données. Tout en offrant un standard élevé, elle est, du fait de son caractère général, suffisamment souple pour tenir compte des différents systèmes juridiques et des diversités propres aux différentes régions du monde. Avec la Convention sur l'intelligence artificielle, la Convention 108+ offre un cadre robuste pour garantir les droits humains et les libertés fondamentales lors du recours à l'IA.

L'évolution actuelle ne paraît hélas pas favorable à la protection des données. En effet, dans un monde dominé par la guerre en de nombreux coins du globe et en particulier sur le continent européen ou au Proche Orient, dans un monde où de nombreuses personnes sont victimes de ces conflits, de la famine ou de la persécution et de la répression et trop souvent obligées de fuir leur terre d'origine, dans un monde où des régimes extrémistes et autoritaires se renforcent ou se mettent en place au détriment de la démocratie et de l'Etat de droit, dans un monde où l'appât du pouvoir et du profit l'emporte sur toutes considérations éthiques et juridiques, les droits humains et les libertés fondamentales et notamment le droit à la vie privée et à la protection des données sont de plus en plus fragilisés. Les politiques de sécurité, à l'exemple de nombreux projets de déploiement de la vidéosurveillance de plus en plus associée à la reconnaissance faciale ou encore des obligations adressées aux fournisseurs de messageries d'abaisser le niveau de chiffrement des données ou de conserver des données relatives aux communications numériques, ne cessent de se renforcer sans qu'on en comprenne et mesure toujours les nécessités et leur efficacité. Le risque d'une dérive vers une surveillance généralisée est devenu bien réel. Or la sécurité des personnes et des biens ne peut se faire aux dépens des droits humains et des libertés fondamentales.

Des oligarques du numérique font pression pour remettre en cause certaines réglementations cadrant le monde virtuel dans lequel nous évoluons. Comme le relève le philosophe Mark Hunyadi¹, l'enjeu du numérique enrichi de l'IA « est d'imposer tendanciellement à tous les humains, dans tous les domaines de leur existence, un rapport au monde qui passe par ses dispositifs techniques, de faire du numérique, pour chacune et chacun, une médiation obligée au monde. » La société sera de plus en plus gouvernée par les algorithmes. Face à ces évolutions, les autorités de protection des données sont sous pression et leur indépendance si fondamentale pour assurer l'effectivité du droit à la protection des données est trop souvent remise en cause.

L'Intelligence artificielle générative est devenue une réalité incontournable. Le recours aux neurosciences en lien avec l'IA est en plein essor. Au côté des avantages indéniables et des perspectives positives pour les êtres humains notamment dans l'accomplissement de tâches rébarbatives ou pour le traitement de nombreuses maladies, l'IA comporte de nombreux risques qui pourraient rapidement déboucher sur un renforcement de la surveillance et du contrôle des activités, des comportements, voire des pensées de tout un chacun et nuire à leur capacité de décision. L'IA prédictive notamment dans le domaine de la criminalité ou de la santé est aussi en plein développement et entraîne de nouveaux défis, en particulier quant à la qualité des données utilisées, pour le respect des droits humains et les libertés fondamentales avec des risques d'injustice, d'atteinte à la dignité et de discrimination. Le risque que les données produites par ces technologies ne soient exploitées par les tenants du « capitalisme de surveillance » lequel tend à influencer et manipuler les comportements et les choix de tout un chacun devient plus que réel. L'IA contribue également à renforcer les politiques de surveillance de masse déployées par certains Etats. « Si l'IA se développe dans des sociétés qui auront été dynamitées dans leur fonctionnement et dans leur capacité à prendre des décisions, tous les avantages de cette technologie, qui sont considérables dans le domaine de la recherche et de la santé notamment, seront annulés. »² Sans volonté affichée des différents acteurs de respecter une éthique respectueuse des droits humains et des libertés fondamentales et notamment le droit à la vie privée, le droit à l'autodétermination informationnelle et la dignité humaine et en l'absence de cadres juridiques contraignants régissant ces technologies, on risque d'ouvrir de manière irréversible la boîte de Pandore.

Alors face à cette spirale négative, le droit à la protection des données a-t-il encore une raison d'être et n'assistons-nous pas impuissants à l'apparition d'un monde où la sécurité et l'ambition de domination et de pouvoir par la technologie justifie toutes les politiques y compris la mise entre parenthèse de l'Etat de droit, de la démocratie et des droits humains ?

¹IA : la bataille de l'esprit, Revue Esprit d'avril 2025

² Interview de Giuliano da Empoli dans le Temps du 5 avril 2025

Tout n'est pas perdu ! Plus que jamais, le Conseil de l'Europe se doit de s'engager fermement pour la promotion et la défense de ses valeurs que sont l'Etat de droit, la démocratie et les droits humains. Cela passe obligatoirement par la promotion du droit à la protection des données et l'intégration des politiques qui y sont liées. La ratification et l'entrée en vigueur de la Convention 108+ sont un impératif urgent qui ne peut plus attendre ! Il en va de même de la Convention cadre sur l'intelligence artificielle.

Au-delà des réglementations et des interventions indispensables des autorités de protection des données, l'avenir de la protection des données passe par la sensibilisation, l'éducation et la formation en particulier des jeunes générations. Dans la mesure où celles-ci pourront intégrer et développer une éthique de la donnée respectueuse des droits humains et des libertés fondamentales, elles pourront à l'avenir promouvoir et bâtir un monde basé sur la confiance mutuelle, respectant l'autonomie informationnelle de tout un chacun.

Au niveau du Conseil de l'Europe, le nouveau règlement de protection des données qui permet à l'organisation de se doter d'un instrument moderne est encore en cours d'implémentation. Le programme de formation des agents devrait finalement débiter. Le défi pour l'organisation malgré ses ressources limitées, est d'octroyer enfin des moyens suffisants pour une application effective et exemplaire de sa réglementation. Le Conseil de l'Europe se doit en effet d'être un modèle s'il veut demeurer un ambassadeur actif et crédible dans la promotion du droit à la protection des données en Europe et dans le monde.

1. Introduction

Le mandat du Commissaire à la protection des données du Conseil de l'Europe a été initialement établi par le Règlement du Secrétaire Général du 17 avril 1989 instaurant un système de protection des données pour les fichiers de données à caractère personnel du Conseil de l'Europe. Par sa résolution CM/Res(2022)14, le Comité des Ministres a adopté le nouveau Règlement du Conseil de l'Europe sur la protection des données à caractère personnel.

Ce nouveau règlement est entré en vigueur le 1^{er} janvier 2023, avec une période transitoire de deux ans pour l'Organisation.

Ainsi, selon la Résolution CM/Res (2022)14, le-la Commissaire à la protection des données en fonction à la date d'entrée en vigueur du présent Règlement continue d'exercer ses missions jusqu'à l'expiration de son mandat, sans préjudice de la possibilité d'être réélu·e conformément aux dispositions du présent Règlement³.

En attendant l'entrée en vigueur de la Convention 108+, le-la Commissaire à la protection des données est élu·e par les représentant·e-s des États membres au sein du Comité de la Convention établi en vertu de l'article 18 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108).

³ Article 3 de ladite Résolution

Le Commissaire actuellement en fonction, Monsieur Jean Philippe Walter, a été élu lors de la 36ème réunion plénière du Comité consultatif de la Convention 108 (Strasbourg, 19-21 juin 2018) et réélu, sous l'ancien régime, en juin 2021 lors de la 41ème réunion plénière du Comité consultatif. Son mandat prolongé d'une année en 2024 s'achève à fin juin 2025 et son successeur-e sera élu-e par le Comité consultatif lors de sa 48ème réunion. Il/elle entrera en fonction le 1^{er} juillet 2025.

En vertu de l'Article 17 du nouveau Règlement, le-la Commissaire à la protection des données prépare et publie un rapport annuel décrivant ses activités. Le rapport doit être présenté pour information audit Comité de la Convention; puis il est transmis au-à la Secrétaire Général-e ; et il est rendu public. Le présent rapport fait état des activités menées entre juin 2024 et mai 2025.

2. Présence physique au siège de l'Organisation et représentation

3.1 Visites au Conseil de l'Europe

Depuis juin 2024, le Commissaire à la protection des données a pu effectuer 3 visites de travail au Conseil de l'Europe. Dans le cadre de ces missions, il a pu rencontrer des agents à leur demande, s'entretenir avec les responsables de divers services, continuant d'entretenir ainsi un dialogue nourri et efficace avec les représentants de nombreuses entités administratives, ainsi qu'avec plusieurs agents impliqués dans le traitement de données à caractère personnel par l'Organisation. Il s'est également entretenu régulièrement avec la Commission du personnel et son président en relation avec des traitements de données relatives aux agents. Il a également rencontré le directeur du cabinet du Secrétaire général, l'occasion de faire un état de la situation en matière de protection des données au sein du Conseil de l'Europe. Il a également eu plusieurs entretiens par visioconférence. Durant la période de référence aucune plainte formelle n'a été introduite auprès du Commissaire.¹⁰ Des demandes, notamment concernant l'exercice du droit d'accès, lui ont été transmises qui ont pu être traitées en premier ressort par la DPO. Il a également demandé des éclaircissements en rapport avec le déploiement de plusieurs outils informatiques ou le recours à l'IA. Il s'est prononcé sur la procédure interne de recrutement du personnel.

Le Commissaire a également publié une déclaration à l'occasion de la 19ème édition de la journée de la protection des données et répondu à plusieurs sollicitations de médias. Il a répondu également à des enquêtes dans le cadre de projet de recherche scientifique.

Durant la période de référence, le Commissaire a continué d'échanger et de collaborer avec le Comité de la Convention 108, sa Présidente et le Bureau du Comité. Il a également pris part à la fin de l'année 2024 à l'échange organisé par le secrétariat relatif à la préparation de l'entrée en vigueur de la Convention 108+, ainsi qu'au séminaire consacré à l'intelligence artificielle et à la protection des données.

¹⁰ Dates des visites de travail : 7-8 octobre 2024, 24-25 février 2025 et 19-20 mai 2025

3.2 Participation à des événements extérieurs

Le Commissaire est régulièrement sollicité afin de participer à des séminaires ou à des conférences, qu'il s'agisse de présenter le cadre interne à l'Organisation ou la modernisation de la Convention 108 (« Convention 108+ ») et les travaux du Comité de la Convention (protection des données et intelligence artificielle, identité numérique, la reconnaissance faciale, etc.). Il a également participé à la réunion annuelle de l'Assemblée mondiale de la vie privée et de la protection des données qui s'est tenue à Jersey du 28 octobre au 1^{er} novembre 2024. A cette occasion, il a présenté très brièvement le nouveau règlement et ses activités. En revanche n'ayant pas reçu les informations y relatives, il n'a pas été en mesure de participer à la conférence de printemps des autorités européennes de protection des données qui s'est tenue en Géorgie au début mai.

4 Conseils et recommandations aux entités du Conseil de l'Europe

Le Commissaire est appelé à émettre des avis ou des recommandations, voire des décisions concernant le respect du droit à la protection des données personnelles à travers différents domaines d'activité ou différentes technologies. Les principaux sujets abordés sont résumés ci-dessous par service/entité concerné(e).

4.1 Direction des Services Généraux

Divers sujets ont été abordés, notamment, la question de la vidéosurveillance, laquelle demeure toujours à l'ordre du jour de la Direction. Le Commissaire consulte régulièrement les registres d'extraction (vidéosurveillance et badge). Lors de sa visite de février 2025, la Direction a informé le Commissaire qu'à la suite d'un audit de sécurité, un renforcement de certaines mesures doit être envisagé. Dans le futur, il n'est pas exclu qu'on recourt également à l'Intelligence artificielle et la reconnaissance faciale. Conformément à l'article 9 du règlement de protection des données, un tel développement devra faire l'objet d'une analyse détaillée de son impact potentiel sur les droits et les libertés fondamentales des personnes concernées avant le déploiement de ces technologies et les traitements qui en découlent devront être conçus de manière à prévenir et minimiser les risques d'atteinte à ces droits et libertés. La nécessité de telles évolutions devra être clairement démontrée. Le cas échéant, l'utilisation de l'IA à des fins de sécurité devra reposer sur un cadre réglementaire spécifique. Le Commissaire appelle cependant à une certaine retenue et à ne pas déployer ces technologies trop rapidement et sans recul au risque de porter atteinte à l'image de l'organisation. En outre, des efforts particuliers sont poursuivis par la Direction conjointement avec la Direction des Technologies de l'Information (*DIT*), pour les bureaux externes du Conseil de l'Europe, avec pour objectif une mise à niveau conforme aux standards de Strasbourg. Pour assurer une unité d'approche sur les mesures de sécurité, le Commissaire est favorable à ce que la responsabilité pour les bureaux externes incombe à une seule entité. De plus se référant à son rapport d'activités juillet 2018 – novembre 2020 (p. 8) et à sa recommandation du 6 juin 2019, le Commissaire rappelle également que le recours à des technologies d'authentification biométrique pour le contrôle d'accès à des locaux du Conseil de l'Europe n'est actuellement pas nécessaire et adéquat au regard des risques encourus. Enfin, le remplacement des badges d'accès qui devrait intervenir prochainement devra respecter ses recommandations antérieures notamment quant à l'émission de badges neutres sans données personnelles visibles à l'œil nu (voir rapport d'activités novembre 2020 – octobre 2022, p. 7). Pour un contrôle d'accès, une lecture de données à la machine est en effet suffisante ; les détenteurs de badges doivent en revanche être clairement informés des données les concernant enregistrées sur le badge et dans le système de contrôle.

4.2 Direction des Ressources Humaines (DRH)

Le commissaire a poursuivi ses contacts réguliers avec la Direction des Ressources humaines.

Il a notamment à nouveau abordé la question de la nouvelle procédure de recrutement du personnel laquelle devrait permettre de limiter la collecte de données personnelles dans la première phase de la procédure en simplifiant le formulaire utilisé. Le recours à l'Intelligence artificielle dans le processus de recrutement a également été abordé. Le Commissaire relève l'importance d'assurer la qualité des données traitées dans le système et salue l'approche de la DRH de maintenir la nécessité du regard humain avant toute prise de décision. L'IA sera utilisée pour procéder au premier tri.

Le Commissaire a également émis un avis relatif à la procédure de recrutement à l'interne. Actuellement pour des motifs de transparence, la liste des candidats est publiée sur le site Intranet du Conseil de l'Europe et toutes les personnes ayant un accès à l'Intranet peuvent la consulter. En outre, le supérieur hiérarchique est informé de la postulation d'un.e subordonné.e. Cette procédure est soutenue par la Commission du personnel qui craint qu'un changement de procédure ne garantisse pas l'équité de la procédure. Pour donner suite à plusieurs demandes d'agents mettant en cause cette pratique, le Commissaire a abordé la question avec la DRH qui lui a demandé un avis. Dans ses premières conclusions, le Commissaire estime que la publication sur Intranet d'une liste nominative des agents ayant postulé lors d'une mise au concours interne ne repose pas sur un intérêt prépondérant à la transparence de la procédure qui l'emporte sur le droit à la protection des données et à la vie privée des personnes concernées, notamment le risque de nuisance aux personnes concernées. L'information du supérieur hiérarchique devrait être effectuée par la personne concernée si elle le souhaite ou avec son consentement au moment où elle le juge opportun. La publication du nombre de candidats retenus après sélection et l'information relative au candidat engagé n'est en revanche pas problématique du point de vue de la protection des données. A la connaissance du Commissaire, une telle pratique n'a pas cours dans les Etats membres ou dans les institutions européennes. Des discussions se sont poursuivies avec la Commission du personnel et la DRH. Suite à son analyse complémentaire, le Commissaire a émis une recommandation à l'adresse de la DRH demandant de ne plus publier la liste des personnes candidates à un poste lors d'un recrutement interne et de mettre en place des mesures propres à assurer le bon déroulement de la procédure. Il parvient à la conclusion que la publication des listes de candidat.e.s ne repose sur aucune base juridique. D'autre part, la publication sur l'Intranet de la liste des candidat.e.s aux avis de vacances internes ne permet pas d'atteindre la finalité recherchée à savoir une procédure de recrutement conforme à la bonne foi, objective et non-arbitraire. Elle est dès lors disproportionnée et la protection des personnes concernées contre un risque d'atteinte à leurs droits l'emporte sur l'intérêt à la publication.

Le Commissaire a été contacté par une agente qui se plaignait d'une collecte excessive de données personnelles dans le cadre d'un remboursement de frais de voyage. À la suite des éclaircissements que le Commissaire a effectués en collaboration avec la DPO, il a été constaté que lors d'un changement de système, des informations non nécessaires au remboursement avaient été effectivement demandées. Ces informations ont été effacées. En outre sur la base de ses constatations, le Commissaire conclut que cette erreur concernait un cas isolé.

Le Commissaire a mené un premier échange avec la Conseillère en éthique de l'organisation, laquelle lui a présenté les aspects principaux de son mandat. La protection des données nécessite une attention particulière de sa part notamment pour préserver la confidentialité et

prévenir des divulgations non autorisées. Il est convenu de poursuivre les échanges et de voir dans quelle mesure une collaboration plus étroite peut être mise en place.

Le Commissaire a participé à une séance du « Well-being Network » mis en place par la DRH. Ce réseau est composé d'acteurs liés au thème du bien-être (conseiller en éthique, DRH, médiateur, CdP notamment), ayant des rôles différents mais qui se chevauchent. Le réseau se réunit régulièrement pour échanger sur les problématiques de l'Organisation et se coordonner sur les actions à mettre en place. Il est appelé à traiter des situations individuelles qui peuvent nécessiter de connaître l'identité des personnes concernées. Les participants ont abordé les aspects de protection des données et de confidentialité qui doivent être garantis de manière robuste. Le Commissaire a insisté sur l'importance du consentement des personnes concernées en cas de partage de données personnelles et préconisé la mise en place d'une charte ou d'un règlement pour le réseau.

4.3 Direction des Technologies de l'Information (DIT)

Le dialogue régulier entre la DIT et le Commissaire s'est poursuivi. L'introduction de l'IA générative au sein de l'organisation est un dossier prioritaire de la DIT qui teste actuellement différents produits. Le Commissaire a eu l'occasion d'assister à une démonstration des potentialités de l'intégration de l'IA dans le traitement de l'information (PV, traduction, rapport, recherche, documentation).

Le Commissaire considère que le recours à l'IA dans le travail de l'organisation ne pourra pas être évité à l'avenir. Une réflexion en profondeur devrait être conduite avant toute décision de déploiement. Il est nécessaire de bien encadrer cette évolution et d'adopter un cadre légal propre à l'organisation qui se fonde sur la Convention cadre sur l'IA. Son recours doit être effectué de manière transparente et les utilisateurs spécialement formés. En outre toute introduction d'un système d'intelligence artificielle doit être précédée et basée sur une évaluation de l'impact potentiel des traitements de données personnelles sur les droits humains et les libertés fondamentales. Il est également nécessaire de définir le seuil des risques admissibles, ce qui implique une gestion des risques et des mesures pour prévenir et minimiser ces risques. Le développement d'une méthodologie dynamique d'évaluation à intégrer dans la gestion des risques est recommandé. Il s'agit de mettre en place une approche structurée de l'évaluation des risques et de l'impact des systèmes d'IA adaptée à la protection des données.

5. Déléguée à la protection des données (DPO)

Durant la période de référence, le Commissaire a collaboré étroitement avec la DPO sur divers sujets. Il lui transmet régulièrement des demandes de clarification à la suite de questions de personnes concernées en relation avec l'exercice de leurs droits. Le Commissaire lui donne également son avis sur différents projets et analyses d'impact relatives à la protection des données. Les échanges sont réguliers sur ces différents sujets.

La mise en place du nouveau règlement demeure la priorité de la DPO. Elle passe par le programme de sensibilisation et de formation des agents dont le lancement est prévu pour le printemps 2025. La cartographie des données traitées (registre des traitements) dans l'organisation a pris du retard, mais demeure une priorité de la DPO. Il s'agit d'un outil important pour assurer la transparence des traitements et notamment faciliter l'exercice des droits des personnes concernées.

Il est rappelé ici qu'aux termes de l'article 11 du règlement, les agents et les autres membres du secrétariat sont tenus de :

- « - traiter toute donnée personnelle avec le plus grand soin ;
- s'abstenir de tout traitement de données à caractère personnel qui n'est pas nécessaire, licite et approprié au regard de leurs devoirs professionnels, du présent Règlement et de ses instruments d'application ;
- demander l'avis du/de la délégué·e à la protection des données, dans des délais appropriés, lorsque le présent Règlement ou les arrêtés, procédures et lignes directrices qui y sont relatives l'exigent ; et agir en conformité avec les recommandations du/de la délégué·e à la protection des données ;
- coopérer à tout moment avec le/la délégué·e à la protection des données et le/la Commissaire à la protection des données ;
- identifier, à leur niveau, et informer rapidement leur supérieur hiérarchique et le/la délégué·e à la protection des données de toute circonstance pouvant entraîner des risques pour la protection des données à caractère personnel. »

Les agent.e.s qui ne respecteraient pas le règlement s'exposent à des sanctions disciplinaires.

Pour être en mesure de respecter ces obligations et qu'ils intègrent au quotidien les exigences de protection des données, il est important que tous les agents suivent le programme de formation et aient accès aux informations pertinentes en matière de protection des données.

La tâche dévolue à la DPO est énorme et le manque flagrant de ressources dont elle dispose nuit grandement à assurer une application effective de la réglementation. Il est urgent que ses ressources soient renforcées.

6. Statuts et organisation du Commissaire à la protection des données

Conformément à la Convention 108+, l'article 15 du règlement précise que le/la Commissaire est une autorité de contrôle indépendante chargée de veiller à la conformité des traitements de données à caractère personnel de l'organisation. Il jouit de pouvoirs d'intervention et d'investigation et notamment d'un pouvoir de décision. A ce titre, le/la Commissaire est chargé(e) notamment de :

- Contrôler et assurer l'application des dispositions du règlement.
- Examiner les réclamations des personnes concernées et ordonner les mesures correctives.
- Mener des enquêtes.
- Formuler des avis à la demande du/de la DPO.
- Faire des recommandations au/à la responsable de traitement.
- Coopérer avec les autorités nationales ou internationales de protection des données, y compris les organisations internationales

Comme indiqué précédemment, il/elle doit également rédiger et publier un rapport annuel sur ses activités. En conformité avec la Convention 108+ et son article 15, même si cela n'est pas expressément mentionné dans le règlement, il/elle doit également pouvoir se prononcer sur

des questions d'actualité en matière de protection des données et donner son avis sur les projets législatifs ou les propositions administratives impliquant des traitements de données à caractère personnel. Ce point devra être précisé lors d'une révision du règlement afin de l'aligner sur la Convention 108+.

Enfin, le/la Commissaire se prononce sur les réclamations des personnes concernées et transmet ses conclusions qui sont définitives et contraignantes au/à la Secrétaire Générale qui doit décider sur cette base. La personne concernée peut recourir contre la décision au Tribunal administratif s'il s'agit d'un membre du personnel, d'un ancien membre du personnel, de ses ayants droit ou d'un candidat à un emploi. Pour les autres personnes qui contestent la décision, un accord à l'amiable doit être recherché et, en cas d'échec, le litige sera soumis à un arbitrage définitif et contraignant.

Les fonctions et les pouvoirs du/de la Commissaire ont été largement renforcés et impliquent un travail de fond et d'analyse du fonctionnement de l'Organisation face à la systématisation du recours aux technologies numériques, y. c. de l'IA dans toutes les tâches et fonctions des agent.e.s tant au siège de l'organisation qu'à l'extérieur. Le système mis en place est en soi robuste et offre toutes les compétences et pouvoirs nécessaires pour veiller au respect des dispositions de protection des données au sein du Conseil de l'Europe. Dans les faits, le/la Commissaire n'est pas suffisamment outillé pour remplir sa mission en pleine conformité avec le règlement. Il intervient sur une base bénévole et ne dispose pas d'un secrétariat correctement doté pour lui fournir le support nécessaire à ses activités. L'Unité de protection des données assure certes de manière professionnelle et dévouée le support au Commissaire ; étant déjà en sous-effectifs au regard des tâches qui lui incombent, elle ne peut cependant lui apporter qu'un soutien très limité, principalement pour l'organisation de ses visites. Cela ne permet pas de procéder à des analyses approfondies ou de mener, comme le règlement, le prévoit des enquêtes ou des contrôles en profondeur des différents systèmes de traitement de données à caractère personnel. Dans la période de référence, ce soutien a encore été plus restreint du fait de changements intervenus au sein du secrétariat et d'absences pour des raisons de santé.

Aux termes de l'article 15 du règlement, le/a Commissaire n'est pas un organe interne du Conseil de l'Europe, mais bien une autorité de contrôle indépendante qui veille à la conformité des traitements de données à caractère personnel effectués par l'Organisation avec les dispositions du règlement. Il doit disposer des ressources nécessaires à l'accomplissement effectif, efficace, et crédible de ses tâches. Il est ainsi indispensable et urgent de doter le/a commissaire des ressources, tant humaines que financières, nécessaires à assurer son secrétariat lequel se doit notamment de préparer les avis, décisions et rapports du Commissaire, d'effectuer des recherches, de le documenter, de procéder aux premières évaluations des demandes qui lui sont adressées, de répondre à des questions diverses ou de le représenter lorsqu'il n'est pas présent ou à sa demande. Le Commissaire devrait disposer de son propre budget. Le Conseil de l'Europe ne peut promouvoir un haut niveau de protection des données à l'extérieur et ne pas avoir à l'intérieur les moyens de garantir le standard de la Convention 108+.

7. Conclusions

L'entrée en vigueur du règlement sur la protection des données a constitué une étape importante pour garantir le respect des droits humains et des libertés fondamentales, notamment le droit à la vie privée des personnes lors du traitement de données personnelles

au sein de l'Organisation. Le délai transitoire de 2 ans pour mettre en conformité les différents traitements est arrivé à échéance en début de cette année. Il reste cependant encore beaucoup à faire, notamment dans la consultation préalable de la DPO et du Commissaire, ainsi que dans les examens d'impact de protection des données qui interviennent encore trop souvent tardivement. Le retard pris dans la formation et la sensibilisation n'a pas facilité le respect de ce délai. Toutefois d'une manière générale, le Commissaire perçoit une meilleure prise en compte des exigences en matière de protection des données et n'a pas constaté de graves manquements aux dispositions du règlement. Vu ses ressources limitées, il n'a cependant pas été en mesure d'effectuer des analyses approfondies des traitements de données à caractère personnel qui lui ont été soumis, ni de procéder à des contrôles.

Il convient à l'avenir de renforcer les moyens allouer au Commissaire et à la DPO en leur octroyant les ressources humaines, financières, matérielles et techniques qui sont indispensables pour assurer l'effectivité de la protection des données au sein de l'Organisation.