

Mise en place d'une gouvernance Informatique et Libertés : un retour d'expérience

Frantz Gourdet

Agence de Mutualisation des universités (AMUE)
Place Ernest Granier
34000 Montpellier

Résumé

À s'aligner sur les exigences établies par la CNIL en décembre 2014 pour son label de gouvernance, les objectifs locaux relatifs à la protection des données personnelles gagnent en exhaustivité et en mesurabilité mais pas forcément en réalisme dans nos établissements.

Le calage de l'organisation interne, la maîtrise d'une méthodologie de mise en conformité des traitements ainsi que la gestion du circuit d'exercice des droits des personnes se révèlent être souvent des voies semées d'embûches et pavées seulement de « bonnes intentions ».

Nous proposons de relater les moyens mis en œuvre pour lever ces difficultés et approcher une « effectivité » raisonnable de la protection des données à caractère personnel.

Analysant les problématiques les plus prégnantes au plan organisationnel, l'article décrit, à titre de retour d'expérience, les grandes lignes et les limites d'une approche à la fois legaliste, managériale et technique où les exigences du label de gouvernance Informatique et Libertés jouent le double rôle de fil conducteur et de levier opérationnel.

Mots-clés

Protection des données à caractère personnel, gouvernance, procédures, relations CIL-RSSI, privacy by design

1 Introduction

Les correspondants *Informatique et Libertés* (CIL) ont été très sollicités depuis la création de cette fonction il y a une dizaine d'années. Leur mission : veiller en toute indépendance au respect des obligations légales incombant aux Responsables des Traitements (RT) en matière de protection des données et de la vie privée des personnes.

Les RT interviennent également dans l'action et la réflexion selon leurs intérêts « légitimes ». Ils déterminent les finalités des traitements et fixent les moyens à engager pour leur mise en œuvre.

Malgré ces deux perspectives distinctes, CIL et RT doivent arrêter ensemble une même démarche opérationnelle à visée legaliste à laquelle participe une kyrielle d'acteurs. L'enjeu demeure la confiance dans l'économie et l'administration numériques.

Mais lors des formalités déclaratives auprès de la CNIL, la « conformité » est encore (trop) vite annoncée. Et pour dépasser ce premier stade d'affichage facial, CIL et RT se trouvent souvent démunis, sans héritage de gouvernance Informatique et Libertés.

Avec son nouveau label institué en décembre 2014, la CNIL livre enfin, en ordre compact, un référentiel qui amorce le déblocage de cette situation. L'article tente de montrer comment, malgré sa faible maturation actuelle sur le terrain, ce référentiel peut nous diriger vers un excellent niveau de protection sans investissements immodérés.

2 Profil de l'organisme étudié

L'organisme faisant l'objet de retour d'expérience est un groupement d'intérêt public (GIP) implanté sur Paris et Montpellier avec un effectif d'environ 150 salariés. Il dispose depuis novembre 2014 d'un CIL interne à temps plein. Ce GIP est *lieu de rencontre, d'échanges et de formation pour la communauté des établissements d'enseignement supérieur et de recherche*. Il se pourrait que, dans certains cas, il faille précisément se reporter à ce contexte, même si les considérations émises dans l'article se veulent d'ordre opératoire général.

3 Choix et suivi des objectifs

En délibération d'adoption [1], la CNIL énonce que la *gouvernance Informatique et Libertés (I&L)* est *l'ensemble des mesures, des règles et des bonnes pratiques qui permettent de préciser les responsabilités qui interviennent dans la gestion des données à caractère personnel en appliquant les lois et règlements*. Et, sur le plan procédural comme sur l'organisationnel, elle dessine avec son référentiel les bases de concrétisation et d'évaluation de la gouvernance ainsi définie. Mais l'ensemble est dense et un supplément méthodologique reste nécessaire pour sa traduction opérationnelle. La suite constitue un mode d'emploi du référentiel « complété » dans ce sens.

3.1 Premiers jalons

Au départ, la priorisation des actions à mener se fait d'elle-même. La vision globale et l'opportunité de fédérer passent après *l'article 31* et l'état des lieux préalable, après le travail de recensement des traitements et l'incontournable registre. En résumé, la charge de mise en conformité aux *dispositions législatives, réglementaires et autres normes dotées de force obligatoire* [1] annihile la Gouvernance avec un grand « G » ainsi que les perspectives qu'offre la quête du label par son côté éthique et responsable. Et lorsque le contrat consiste à persuader une organisation entière de s'atteler à tout un programme non inscrit dans son ADN, l'absence de plan global dès le démarrage de l'aventure peut être à l'origine de stress et d'échec.

Ainsi, la qualité de la gouvernance dépendra des moyens dont disposera le CIL pour s'extirper de cette gestion de l'urgence. L'emploi d'indicateurs simplissimes, propres à la vulgarisation, sera aussi un facteur de réussite. Pour la sensibilisation préalable du responsable des traitements, ces indicateurs devront respecter des critères de pertinence et d'efficacité supposant une économie de moyens lors de leur mise en œuvre.

Actuellement, ni de tels indicateurs ni les outils qui en assureraient l'exploitation ne sont publiés par la CNIL. On ne les retrouve pas non plus, sauf erreur, sur les réseaux de CIL. Cette rareté motive la mutualisation des résultats obtenus sur ce front.

3.2 L'espace de gouvernance

Le référentiel comporte vingt-cinq exigences couvrant les trois thématiques suivantes :

- L'organisation interne dévolue à la gestion des données personnelles ;
- La conformité aux contraintes légales ;
- Le mode de gestion des réclamations et incidents.

Chacune de ces thématiques constitue un sous-espace de gouvernance à examiner séparément en utilisant un même formalisme. Pour évaluer les avancées dans chaque sous-espace, nous avons retenu quatre vecteurs à projeter sur un même plan : les vecteurs du droit et du référentiel, d'un côté et ceux des objectifs et de la réalité, de l'autre. Les deux premiers s'adressent à l'ensemble des établissements et les deux autres caractérisent chaque organisme en particulier. Leurs projections se prêtent à l'observation sous la forme de radars obtenus en utilisant le référentiel CNIL comme base de comparaison. L'ensemble forme un indicateur de gouvernance relatif aux exigences portées en étiquette aux sommets extérieurs de la toile des radars (Fig. 1).

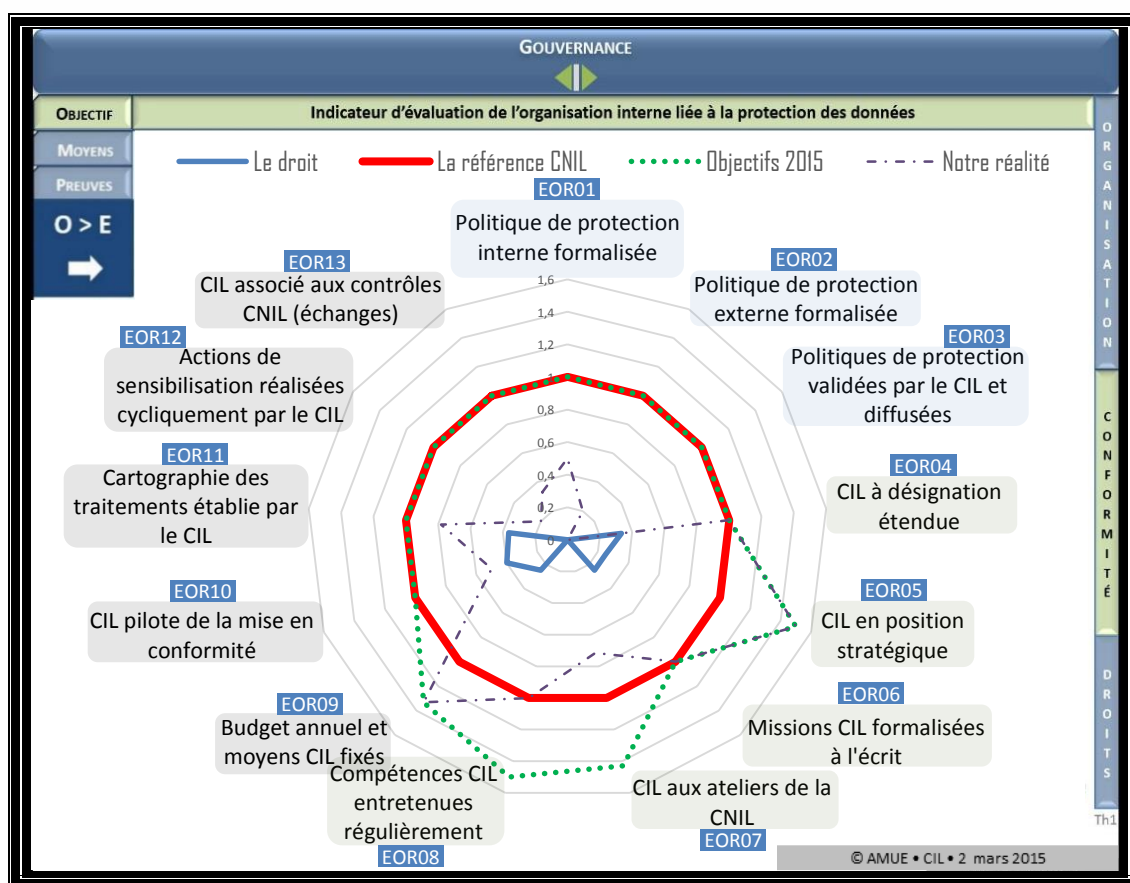


Figure 1 - Indicateur de gouvernance liée à l'organisation : positions relatives des radars.

Le radar du droit schématise les contraintes légales qui s'imposent aux organismes disposant d'un CIL. De manière générale, le radar des objectifs enveloppera le radar du droit (approche légaliste). Sur un axe donné, il se situera en-deçà ou au-delà du radar référentiel ou encore au même endroit que ce radar selon qu'il vise un niveau d'exigence inférieur, supérieur ou identique au référentiel CNIL. La position d'un radar résulte de ses abscisses sommitales c'est-à-dire de la distance de ses sommets au centre de l'indicateur. L'abscisse d'un sommet s'obtient en

divisant le nombre d'items qui lui est associé par le nombre d'items¹ liés à l'exigence qui lui correspond dans le référentiel. De ce fait, les abscisses sommitales du *radar référentiel* valent toutes l'unité et, quelle que soit la dimension du sous-espace de gouvernance examiné, ce radar sera toujours un polygone régulier. Les abscisses des autres radars proviennent des validations et invalidations d'items opérées lors des réunions de suivi. Le *radar de réalité*, par exemple, tend ainsi progressivement vers le *radar des objectifs* par concaténations successives d'items satisfaits/réalisés. Le restant à faire s'évalue en considérant la position du *radar de réalité* par rapport à celle du *radar des objectifs*.

3.2.1 Vision 360°

Dans toute la suite, la situation de l'organisme étudié sera commentée à la date d'observation du 2 mars 2015, date à laquelle cette démarche a été officiellement lancée. Cela mettra en évidence la faculté de dégager, depuis le commencement, une vue d'ensemble utile à l'appropriation de la démarche de gouvernance. Le propos est d'illustrer le fonctionnement de l'outillage conceptuel créé et non d'exposer le détail de tous les résultats obtenus.

3.2.2 De l'organisation interne

Les axes d'exigences organisationnelles du référentiel de la CNIL sont au nombre de treize. On atteint précisément la norme organisationnelle au sens du label lorsque l'on cumule pour cette thématique la satisfaction de la *checklist* complète des exigences abrégées par les « étiquettes » de la *Figure 1*. Il est à remarquer que le cumul en question fonctionne en mode 0 ou 1, sans aucune gradation dans l'évaluation de la qualité de l'organisation. Celle-ci répond (1) ou pas (0) à tel axe d'exigences.

La thématique liée à l'organisation interne s'avérant très « fournie » en exigences, nous la subdiviserons en trois sous-thèmes de moins de sept axes : « Politiques de protection », « CIL » et « Pilotage » (*Fig. 2a, b, c*).

3.2.2.1 Politiques de protection

Objectifs, réalité et droit

L'indicateur dessiné sur la *Figure 2a* dit bien que l'organisme étudié souhaite répondre aux trois premières exigences du référentiel [1]. Celles-ci portent sur la communication autour de l'organisation en matière de protection des données à caractère personnel. Sur cette figure, le *radar du droit* reste introuvable. En effet, il n'est pas (encore) obligatoire en France de publier ni de formaliser des politiques² de protection de données personnelles. L'objet de la réflexion est en premier lieu de rassurer et d'entretenir la flamme de la confiance dans le processus de collecte et de traitement. Tout premier balbutiement d'*accountability*³, cette réflexion animée par le CIL implique les « valeurs » de l'organisme et les grands principes de protection des données et de la vie privée ([3], art. 6). Ces principes doivent impérativement se retrouver dans les documents de formalisation des politiques dont la finition gagne à être l'œuvre concise d'un spécialiste de la communication puisque destinée à véhiculer l'image de l'organisme ([1], *EOR01 et EOR02*).

¹ Les *items* représentent des conditions élémentaires isolables à remplir pour satisfaire une exigence.

² À ne pas confondre à ce stade avec les PSSI (Politiques de sécurité des systèmes d'information).

³ Démonstration aux personnes concernées du caractère responsable de l'organisme et de la conformité des traitements effectués sur leurs DCP.

Donnons à présent l'exemple d'un décompte d'items puisque la démarche repose sur leur identification et leur réalisation. La première exigence n'a qu'un item : « Avoir formalisé une politique de protection des données en interne ». Cet item comporte deux composantes : « Organisation (Rôles, responsabilités) » et « Grands principes ». Au 2 mars 2015, les grands principes sont acquis mais seuls les rôles et responsabilités du RT et du CIL sont entièrement précisés, ce qui est estimé à environ 20% de la mise en place complète de l'organisation⁴. La deuxième exigence renferme deux items : « Politique externe » et « Information claire, accessible et en langue française ». La situation relative au premier item est à mi-chemin de celle de la « Politique interne ». Aucune rédaction n'est encore proposée et, partant, pas d'évaluation pour le second item⁵. La troisième exigence contient trois items (à décliner en interne et externe) : « Validation », « Diffusion », « Périodicité de la validation ».

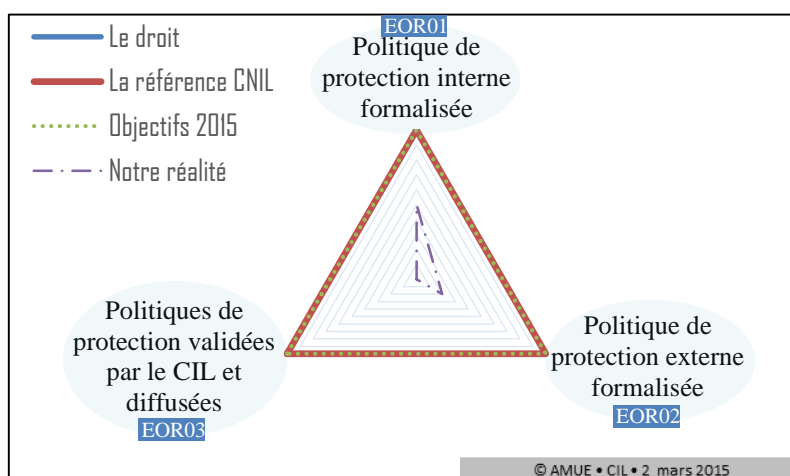


Figure 2a – Indicateur « Politiques »

partant, pas d'évaluation pour le second item⁵. La troisième exigence contient trois items (à décliner en interne et externe) : « Validation », « Diffusion », « Périodicité de la validation ».

Pour le label

Sur le dossier de demande de délivrance du label de gouvernance I&L, les moyens indiqués comme répondant à l'intégralité des items d'une exigence doivent trouver chacun une équivalence en justificatif ([5], § 3.1). A titre indicatif, voici les preuves soumises à la CNIL pour les six items de la thématique des politiques : copies des deux documents de politique de protection (interne et externe) ; lien Internet pour donner à la CNIL la possibilité d'accéder à la politique externe en français ; références exactes aux cartouches des documents de politique (pages et alinéa) indiquant la périodicité et l'auteur de leur validation ainsi que les copies d'écran de leur publication intra et extranet.

3.2.2.2 CIL

Objectifs, réalité et droit

Dès le départ, l'organisme étudié a consenti à renforcer quatre des six axes du référentiel se rapportant aux compétences du CIL (cf. EOR04-EOR09) :

1. Positionnement stratégique :
 - CIL directeur de projet (deuxième niveau le plus élevé de la grille de fonctions) ;
 - Rattachement direct et exclusif au directeur de l'organisme ;
 - Réception formelle du CIL par le RT toutes les trois semaines ;
2. Suivi de la totalité des dix ateliers CNIL et non pas des seuls sept imposés par le label ;
3. Recherche de la maîtrise des systèmes d'information ainsi que des domaines juridiques liés à l'Informatique et aux Libertés (au-delà de l'entretien régulier des compétences) ;

⁴ L'abscisse du *radar de réalité* sur cet axe « Politique de protection interne formalisée » est par conséquent 0,60 (0,5 x 0,20 + 0,5).

⁵ D'où une abscisse de 0,15 (0,5 x 0,60/2 + 0,5 x 0)

4. Budget et autres moyens :

- Budget annuel en adéquation avec les missions et dont le CIL arrête seul les décisions d'utilisation ;
- CIL à temps plein placé en fonction transverse à tous les services *sur lesquels il exerce une autorité fonctionnelle concernant les sujets Informatiques et Libertés se traduisant notamment par l'accès à toute information en lien avec l'exercice de ses fonctions* ;
- Pouvoir de communiquer avec toute personne, hors (et quelle que soit sa) hiérarchie ;
- Obtention en tant que de besoin de la collaboration du RSSI (Responsable de la Sécurité des Systèmes d'Information), du département de production de l'offre SI externe, du service des ressources informatiques internes et logistiques, du pôle communication et du service juridique.

Le 2 mars 2015, au moment de la décision d'utiliser toutes les exigences du label comme fil conducteur, la situation était celle conceptualisée sur la *Figure 2-b*. Il y apparaît que les exigences CNIL étaient déjà satisfaites, hormis celle du suivi des sept (7) ateliers indispensables pour le label, deux (2) d'entre eux devant être dispensés après le 2 mars.

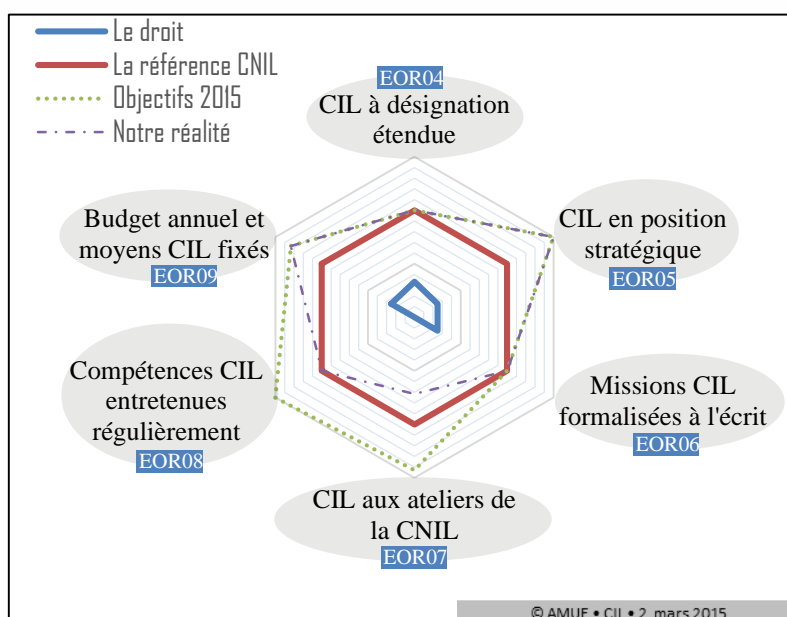


Figure 2b - Indicateur « CIL »

Les premiers objectifs ont finalement été atteints le 9 juin 2015.

Les ateliers sont l'occasion d'illustrer le mode de calcul des abscisses servant à placer les radars. Ce calcul s'effectue en décomptant les items liés au type de radar que l'on veut positionner (droit, objectif ou réalité). Ce nombre est ensuite ramené au nombre d'items exigés par le référentiel. On obtient ainsi, sur l'axe d'exigences 'Ateliers CNIL', les abscisses 0, 1, $10/7^{\text{ième}}$ et $5/7^{\text{ième}}$ pour les radars *droit*, *référentiel*, *objectifs* et *réalité* respectivement. Ces abscisses sont traitées à l'aide d'un outil complémentaire. Pour le *radar de réalité* par exemple, elles résultent de la validation des différents items du référentiel et des suppléments issus d'objectifs de dépassement. Ainsi, c'est en entérinant ou en invalidant l'atteinte de tel objectif ou la satisfaction de telle exigence, par cumul, item après item, que le comité de pilotage fait évoluer la position de ce radar.

Enfin, l'allure du radar central rappelle le statut que confère en son état actuel le droit au CIL ([3], *art. 22* et [4], *art. 42 à 55*).

Pour le label

La lettre de mission (LM) du CIL a servi de justificatif à plusieurs moyens évoqués avec cependant l'indication à chaque fois de l'alinéa de la LM correspondant au moyen en regard ([5], § 3.1). Sur le conseil de prédécesseurs ayant déjà passé le cap de la recevabilité, ce justificatif a été renforcé et/ou complété :

- Pour l'EOR04, par la page de désignation du CIL de l'extranet des correspondants <https://www.correspondants.cnil.fr/cils/secure/designationCorrespondant> ;
- Pour l'EOR05 et son item « Réception formelle périodique », par la photocopie de la série de RDV de l'agenda électronique du CIL ; de même, l'item « rattachement » déjà couvert par des alinéas de la LM, a été renforcé par l'organigramme et la grille de fonctions en raison des dépassements de référentiel annoncés ;
- Pour l'EOR07, par les attestations de présence à tous les ateliers CNIL ;
- Pour l'EOR08 et ses items « Entretien des compétences » et « Régularité/Périodicité », par des attestations de présence en 2014 et 2015 à des formations spécifiques autres que les ateliers CNIL ainsi que le plan de formation 2016 ;
- Pour l'EOR09 en justification de l'item « Budget », par la décision de délégation de signatures indiquant le montant du budget accordé et par un état de l'exécution budgétaire en lien avec l'item « Adéquation budget-missions » (le temps plein et les moyens humains alloués étant attestés par la LM).

3.2.2.3 Pilotage

Objectifs, réalité et droit

CIL pilote de la mise en conformité et associé aux contrôles CNIL... Cartographie établie pour les traitements, actions de sensibilisation réalisées cycliquement... tels sont, selon la Figure 2c, les exigences du label liées au pilotage ([1], cf. EOR10-EOR13). Ces exigences coïncident avec les objectifs fixés par l'organisme étudié. Mais, à la date du 2 mars :

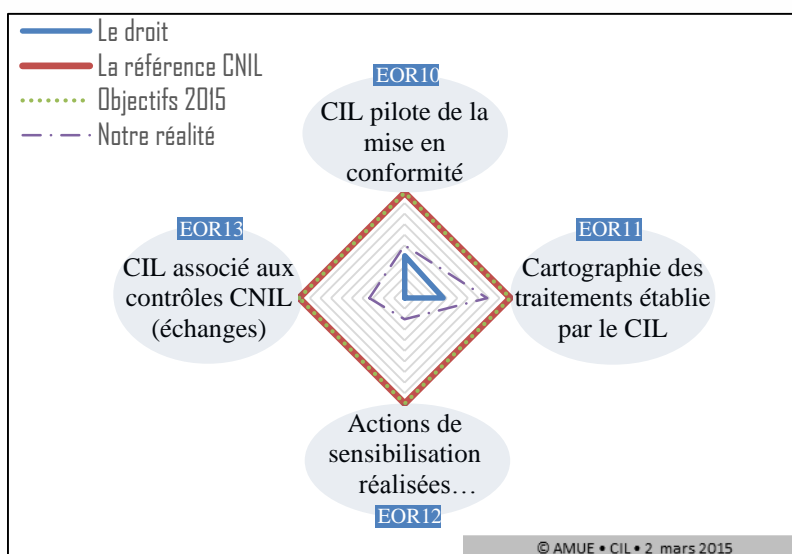


Figure 2c - Indicateur « Pilotage »

- Les comités de pilotage Sécurité RGS et I&L intégrant le CIL viennent d'être créés ;
- Le bilan annuel d'activités peut attendre encore neuf mois (CIL nommé seulement en novembre 2014) ; un outil méthodologique de pilotage est proposé par le CIL mais attend d'être évalué (et d'autres restent à définir) ;
- Le réseau de Relais Informatique et Libertés (RIL) n'est pas encore sur pieds ;
- La mise en œuvre effective du principe de *Privacy by design* ne peut donc pas encore s'appuyer sur ce réseau. Il est d'ores et déjà prévu cependant d'installer dans la pratique courante l'information obligatoire du CIL pour consultation, en cas de collecte ou traitement de données à caractère personnel.

De son côté, le droit n'exige pas (pour l'instant) que les CIL pilotent la mise en conformité. Ce serait même plutôt l'inverse selon la doctrine de quelques-uns qui se réfèrent à l'article 46 du décret d'application du 20 octobre 2015 [4] : il y aurait conflit d'intérêts, surtout dans le cas d'un CIL à temps plein. En réalité, le terme « pilote » est mal choisi et ne doit pas être pris dans son acception de « dirigeant » mais dans celle de « guide » comme le confirme les articles 36 et 37 du projet de règlement européen impliquant le Data Protection Officer⁶ dans un rôle de contrôleur et de conseiller. En tout état de cause, le CIL évitant d'accepter toute délégation formelle de pouvoir du RT en matière I&L sera plutôt couvert par l'art. 46 [4].

Par ailleurs, concernant la cartographie des traitements, le référentiel n'exige pas moins de trente-trois items (33) alors que l'article 48 du décret d'application [4] n'en réclame que douze⁷. Au 2 mars 2015, la cartographie est déjà finalisée pour 69,6 % des traitements. Elle a été établie par extension du registre déjà constitué le 13 février 2015, trois mois après la désignation du CIL répondant en cela à une obligation légale⁸ ([4], DA art.48).

Au terme de la lecture de la Figure 2c, notons encore quelques éléments expliquant la position du radar de réalité :

- Certaines actions de sensibilisation du personnel doivent encore être réalisées ;
- Le CIL est associé – sur le papier – aux échanges avec la CNIL en cas de contrôle. Mais, au 2 mars 2015, il reste à définir les règles d'accueil de la délégation de contrôle et les circuits d'échanges d'information.

Pour le label

On a procédé comme aux §§ 3.2.2.1 et 3.2.2.2 c'est-à-dire par isolation des items et indication des moyens et preuves en adéquation avec chacun d'eux.

3.2.3 Assurance de la conformité

Le langage des radars « exprime » rapidement l'état de la thématique d'assurance de la conformité (Fig. 3). En réunion d'avancement de gouvernance *Informatique et Libertés*, l'indicateur parle de lui-même. Les commentaires viennent seulement répondre à des demandes de précision :

- Les objectifs collent aux attentes du référentiel ([1], EM01 à EM06)
- La phase de régulation des anciens traitements ainsi que des formalités déclaratives s'y rapportant est close ; mais le dispositif complet de mise en conformité en prévision des demandes de conseil pour tout nouveau traitement, à la fois sur le plan juridique et sécurité technique (et physique) n'est pas encore en place ;
- Le plan d'actions préventives ou correctives n'est, dès lors, pas finalisé bien que les recommandations relatives à la régularisation des anciens traitements soient déjà disponibles ;
- La démarche sécurité au regard des risques (*obligation normative pour les organismes publics depuis le RGS...* pourrait préciser utilement, pour certains, le RSSI ou l'AQSSI) est en cours d'élaboration ;
- Il n'est pour l'instant pas prévu d'audit de conformité mais le label exige d'inclure cette perspective dans la procédure de gouvernance.

⁶ DPO, CIL v. 2.0 défini à l'art. 35 du projet de règlement [2]

⁷ D'où une distance au centre de 12/33^{ième} soit env. 0,36 pour le radar du droit au regard de l'exigence « Cartographie des traitements établie... »

⁸ On vérifiera aisément la distance de $0.696 + 0.304 \times 12/33$ soit env. 0,81 pour le radar de réalité

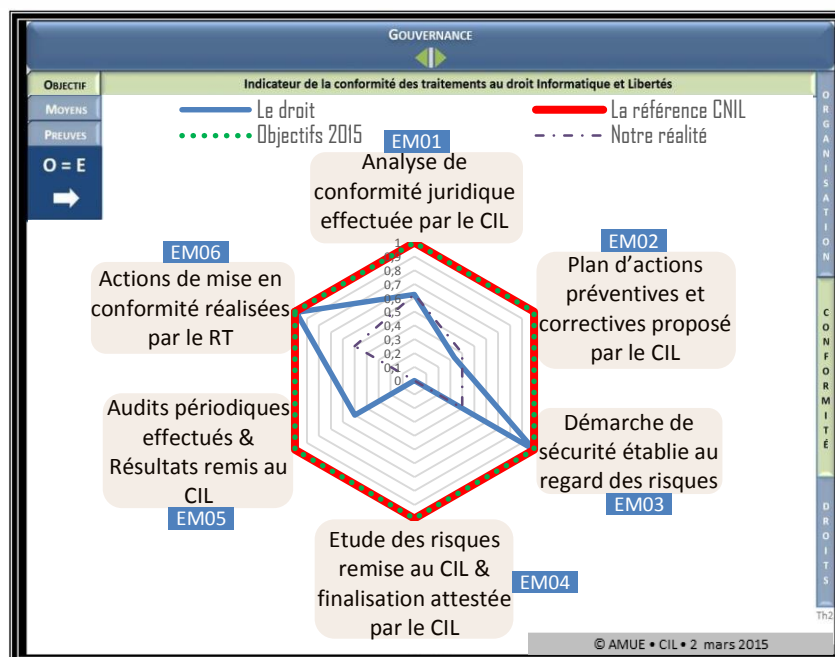


Figure 3 - Indicateur « Conformité ».

Le droit prévoit l'analyse de conformité ([3], LIL art. 6, 7, 32 38, 39, 40, 68 et 69 et Directive-95-96 art. 6, 10, 11, 12, 14, 25 et 26) mais pas explicitement d'actions préventives et correctives proposées par le CIL. Le droit exige les actions de mise en conformité réalisées par le RT ([3], LIL art. 34) ainsi qu'une démarche de sécurité au regard des risques et donc l'étude de ces risques (cf. RGS) mais pas que les documents formalisant l'étude et la démarche soient – obligatoirement – remis au CIL.

Après la régularisation de l'existant, il a découlé – et découle toujours – des exigences EM01 à EM04 la nécessité de conduire une étude d'impact sur la vie privée en amont de tout nouveau traitement. Et les exigences EM05 et EM06 amènent à réexaminer périodiquement les traitements les plus sensibles.

Examen d'impact a posteriori – Régularisation

Dans un contexte de reprise de l'existant, la réalisation de la cartographie selon l'EOR11 a constitué un excellent levier de régularisation. En effet, de la dénomination du traitement à l'utilisation des *cookies* en passant par l'exercice des droits et la sécurité, chacun des dix-sept volets de cette cartographie (cf. onglets Fig. 4) fait l'objet d'une confrontation entre réalité, d'un côté et contraintes légales et exigences du label, de l'autre. Tout constat de défaillance est tracé (cf. exemple Fig. 4) et entraîne des recommandations du CIL et un plan d'actions correctives.





N°4	RESPONSABLE	FINALITÉS	MISE EN ŒUVRE	EXERCICE DROITS	MODALITÉS EXER	DONNÉES	CONCERNÉS	DESTINATAIRES
	CONSERVATION	RÉG. JURIDIQUE	SÉCURITÉ	TRANSFERTS	SOUS-TRAITANCES	RISQUES	CONSENTEMENT	COOKIES
CARTE EOR11 – GESTION TITRES RESTAURANT 								
Les commandes de titres restaurant sont passées à la société [REDACTED]								
EXIGENCE (art. 35 LIL)							RÉALITÉ	
Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.								
Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement								
© AMUE • CIL • 2 mars 2015 								

Figure 4 - Cartographie EOR011 - Volet « sous-traitance » d'un traitement : les traces avant régulation sont conservées (Boutons rouges: détails points non-conformes - Flèches vertes du bandeau supérieur : évolution de la conformité dans le temps).

Impact amont - Anticipation

Mais au-delà de la régularisation de reprise d'existant, la satisfaction des exigences allant de l'EM01 à l'EM04 implique d'examiner la conformité de manière systématique et structurée à l'amont de tout nouveau traitement afin de pouvoir respecter les grands principes et les droits fondamentaux des personnes concernées et de déterminer les mesures techniques et organisationnelles de protection effective adaptée au contexte de l'organisme. Cette étude d'impact spécifique I&L est à mener au plan juridique, d'une part et au plan de la sécurité des DCP, d'autre part (confidentialité, intégrité et disponibilité).

Impact Aval - Périodicité

De même, à l'aval, une fois le nouveau traitement mis en place, s'il compte parmi les plus sensibles, on lui applique périodiquement *a posteriori* le même examen de conformité qu'à l'amont.

Un visa bienvenu

À la date d'observation du 2 mars, les guides de *Privacy Impact Assessment* (PIA) font encore défaut. Ils arriveront finalement en juin 2015 pour préciser la méthode de gestion des risques sur les libertés préconisée par la CNIL et agréer une étude d'impact sur la vie privée avec un visa clair. L'organisme étudié a aussitôt annexé ces guides⁹ à sa procédure de gouvernance et s'y reporte pour traiter la thématique de conformité.

PIA, Privacy by default/design

La généralisation des études d'impact sur la vie privée (EIVP/PIA) à l'amont de la mise en œuvre des traitements conduit à des solutions logicielles déjà conformes aux contraintes légales à la

⁹ http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-1-Methode.pdf
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-2-Outillage.pdf

livraison et qui évitent, de par leur conception même, la rupture de la chaîne de conformité en phase d'exploitation.

Pour la construction de son offre SI, l'organisme étudié comprend l'importance que revêt le *Privacy by design* c'est-à-dire la prise en compte de la protection des données dès la conception (et même, dès l'évocation des finalités motivant la volonté de traitement). Il inscrit à son programme :

- De respecter ce principe de *Privacy by default/design* sur toute la durée de vie des logiciels, par exemple :
 - en phase de maintenance curative ou évolutive ou lors des tests en masse sur données réelles ou *anonymisées* des établissements ;
 - pour une meilleure gestion de la problématique de durées de conservation ;
 - avec un paramétrage par défaut conforme au droit et, par exemple, des dispositifs de création de liens vers les politiques de protection propres à chaque établissement voire, au besoin, vers la fiche de registre du traitement concerné, faisant ainsi de l'*accountability* une réalité immédiate en répondant au « toujours plus connectés » par un « encore plus accessibles » ;
 - en protégeant les « contenus » aussi bien que les contenants (Impossibilité d'avoir des mots-de-passe ou des DCP sensibles stockés en base sans hachage).
- D'incorporer des paragraphes Informatique et Libertés dans son dispositif d'assurance qualité pour tout domaine d'activités « consommant » des données à caractère personnel (sont ainsi concernés : le « kit des marchés publics », les modèles de CCTP, les procédures d'expression des besoins et de validation des contrats de sous-traitance) ;
- De diffuser sur l'extranet l'analyse du régime juridique applicable et le rappel des formalités déclaratives à effectuer ainsi que des fiches de registre types pour chaque produit de l'offre SI ;
- De mettre à jour le « Guide Informatique et Libertés pour l'Enseignement supérieur et la Recherche » (Amue, CNIL, CPU) dès la parution du prochain règlement européen ;
- D'accompagner les établissements dans leur démarche de gouvernance Informatique et Libertés dans la perspective du futur règlement, en lien avec la CPU (formations, fourniture d'outils méthodologiques)...

Relation CIL-RSSI pour la conformité

Un PIA boucle sur quatre étapes d'examen portant sur : le contexte, les mesures (juridiques et de traitement technique, physique et organisationnel des risques), la qualification de ces risques (gravité, vraisemblance) et, finalement, après évaluation de l'acceptabilité ou pas de la façon dont il est prévu d'agir sur les risques, l'arbitrage entre l'application du plan d'actions ou sinon la révision des objectifs (avant d'examiner le nouveau contexte et ainsi de suite).

Afin que soit assurée la mise en conformité des traitements et la protection technique et physique des DCP, le CIL informe le RSSI sur le contexte et les enjeux des traitements et les mesures prises ou à prendre pour respecter les contraintes légales I&L. Mais, pour ce qui a trait à la sécurité technique et physique, il attend du RSSI :

1. L'inventaire des mesures existantes/prévues pour traiter les risques sur la vie privée de manière proportionnée ;
2. L'identification des sources de risques sur les DCP (motivations/mobiles possibles et profil d'attaque) en connaissance des limites du système d'information ;
3. Des informations pour lister les événements redoutés et en déterminer la gravité ;

4. Le signalement des menaces liées à ces événements (modes opératoires probables etc.) et leur vraisemblance ;
5. Toutes autres informations facilitant l'évaluation et la vérification du mode de traitement des risques.

Aux autres intersections de la sécurité générale et de la protection spécifique des données personnelles, le CIL attend du RSSI les documents visant à démontrer la conformité au RGS de la politique sécurité appliquée dans l'organisme et répondant à l'article 34 de la loi Informatique et Libertés. En fonction de l'étape atteinte pour le SMSI¹⁰, il s'agit notamment de : la *Note d'engagement d'implémentation*, la *Définition du périmètre initial* et le *Plan projet d'implémentation* ainsi que la *Politique de gouvernance*, la *Stratégie de gestion des risques*, la *Listes des mesures de sécurité existantes*, *Analyse de risque*, *Plan de traitement des risques*, *Déclaration d'Applicabilité*, *Projets de sécurité*, *Politique de Sécurité et procédures liées à la sécurité*, les *Procédures SMSI* et les *Rapports d'audits internes*.

En cas de divergence sur ces rôles respectifs, c'est la hiérarchie des textes définissant séparément les responsabilités de chacun des acteurs qui tranche. Mais, au-delà de cette réponse primordiale visant positionnement de droit formel, l'essentiel est d'établir un partenariat CIL-RSSI fécond et de tirer le meilleur parti des compétences de chacun.

3.2.4 Réclamations et incidents

Les objectifs correspondent aux exigences du référentiel (Fig. 5).

Les procédures de suivi de l'architecture de journalisation des événements sécurité, de gestion et de notification des violations aux personnes concernées sont incluses dans la PSSI de l'organisme et concernent le RSSI au premier chef ([1], EG01-EG06).

Cependant, pour être au niveau de « labélisable », il est obligatoire d'élaborer une procédure spécifique de gestion des violations de données prévoyant notamment ([1], EG05) :

- *L'information du CIL dans un délai inférieur à 24h à partir de la détection de la violation ;*
- *La formulation des recommandations du CIL et leur transmission au responsable de traitement ;*
- *La réalisation des actions correctives et l'information du CIL ;*
- *Une notification aux personnes concernées dans un délai inférieur à 72h en cas d'accès par un tiers non autorisé à des données personnelles.*

Autant d'éléments restant au 2 mars 2015 à être intégrés par le RSSI dans ses procédures. A cette date, une architecture de journalisation des événements sécurité existe mais n'intègre aucun dispositif particulier pour les DCP et le plan de contrôle de la politique de traces n'est pas encore mis en œuvre.

Quant à la procédure de gestion des réclamations, elle se résume à l'époque à une adresse de contact aboutissant au CIL avec le délai de communication comme unique item (sur trois) de précisé pour cette exigence et ce, par contrainte légale ([4], art. 94) : Pas de modalités d'exercice ni de chaîne de traitement ni encore de référencement sur l'intra ou l'extranet de courriers types tirés par exemple du « Guide droit d'accès » de la CNIL¹¹.

¹⁰ <http://www.iso.org/iso/fr/home/standards/management-standards/iso27001.htm> et RGS - Système de Management de la Sécurité de l'Information

¹¹ http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf

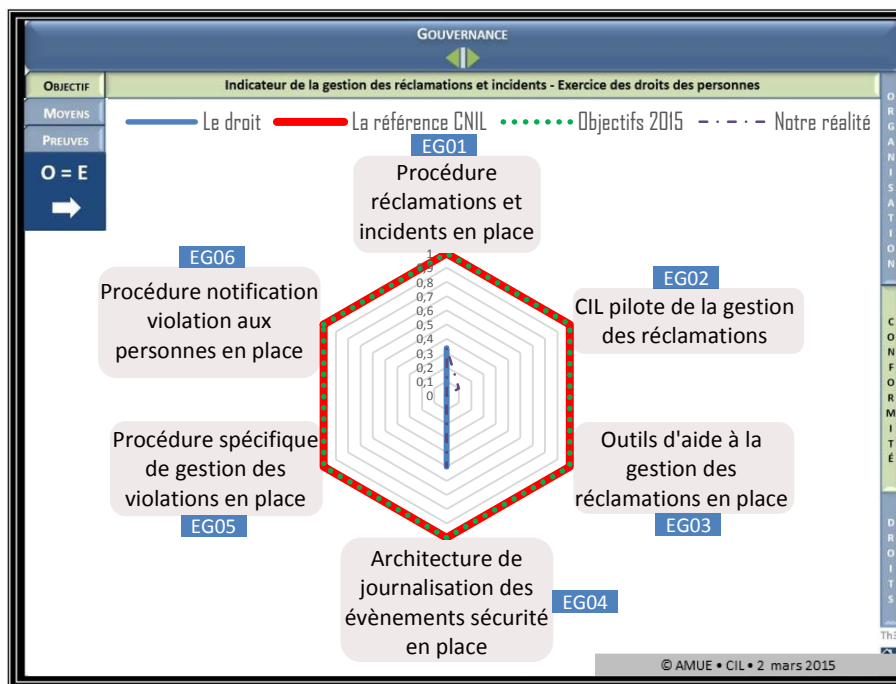


Figure 5 - Indicateur « Réclamations et Incidents ».

4 Vers la réalisation des objectifs

Le référentiel fourni par la Commission Nationale établit la liste que l'on peut considérer comme suffisante du « quoi obtenir » mais non pas du « comment y aboutir ». Cela se conçoit bien puisque ce « comment » dépend du contexte et des ressources locales. Chaque étape, chaque objectif prend l'allure d'un projet de construction dont il faut à la fois livrer (ou contrôler) les plans d'exécution et piloter la concrétisation.

Pour les plans d'exécution, les compétences techniques et juridiques du CIL s'avèrent indispensables, bien qu'il soit plutôt conseillé de s'appuyer sur des partenaires spécialisés.

Pour le pilotage, les compétences organisationnelles et de communication sont sollicitées.

L'outillage déployé comprend :

- L'indicateur *zoomable* sur la thématique de gouvernance souhaitée ;
- Une méta-fiche projet où l'instance décisionnelle est le RT au sommet de la hiérarchie ;
- Une fiche projet par exigence à mettre à jour à chaque réunion de travail.

Chacune de ces fiches est munie d'indicateurs d'avancement et conserve l'historique :

- Des difficultés/risques, scénarii de résolution et points soumis à arbitrage ;
- Des décisions prises ;
- Des actions planifiées suite aux décisions, des acteurs concernés et des échéances ;
- Des items/actions réalisés depuis le dernier point et des actions en cours.

5 Récapitulatif par le prisme de l'outillage

5.1 Gestion des items

L'outillage de gouvernance sert à saisir les items du référentiel et à effectuer pour le *radar du droit* un paramétrage initial. L'étape suivante consiste à définir le *radar des objectifs* à partir des

items du référentiel en cochant ceux que l'on souhaite s'imposer. On en rajoute si l'on vise plus haut. La position du *radar de réalité* évolue en fonction des nouvelles valeurs de ses abscisses recalculées à chaque validation s'opérant en cochant les items réalisés.

5.2 Navigation

À partir du menu d'accueil, on accède aux trois thématiques : organisation, mise en conformité, gestion des réclamations et incidents. Chaque indicateur donne accès à des fiches de description détaillée des exigences et des objectifs. Il suffit de cliquer sur les « étiquettes ». Ces fiches descriptives sont munies de boutons de consultation des items et des moyens associés. Le référencement des preuves au dossier de demande de labélisation est également possible. Parmi ces moyens et preuves figure la cartographie EOR11 à partir de laquelle on explore chacun des dix-sept volets (et trente-trois items) de chaque traitement. Il faut aussi compter avec les fiches projet déjà évoquées où les items sont exploités sous forme d'actions préenregistrées réalisées ou à réaliser. Ses items-actions mis ainsi en relation avec les points d'arbitrage et les décisions sont alors affectés d'acteurs, de délais de réalisations et au besoin de poids financiers.

Ainsi, le référentiel décomposé en exigences, elles-mêmes subdivisées en items à leur tour découpés s'il y a lieu en étapes, actions, tâches, critères etc... constitue le fil conducteur de toute la démarche. Ce référentiel agit alors comme un méta projet qui se démultiplie en autant de sous-projets qu'il est nécessaire de conduire afin d'atteindre l'ensemble des objectifs. Et c'est dans ce contexte que se concrétise le pilotage par le CIL de la mise en conformité. Tout au long de la trajectoire, l'outillage de gouvernance aide l'ensemble des acteurs à progresser vers la cible que l'organisme s'est lui-même imposée.

5.3 Implantation de l'outillage

La mise en œuvre crayon-papier de l'outillage décrit ci-dessus débouche très vite sur une impossibilité. Par contre son expérimentation sur la base d'un couple basique MS Excel-PowerPoint (ou équivalent open source) est parfaitement envisageable.

Son implantation logicielle en mode SaaS pourrait amener une gestion mutualisée des items du référentiel et du *radar du droit* et faciliter l'affectation de poids financiers aux items pour calculer les coûts de la conformité.

5.4 De l'indicateur

L'indicateur livre son plein potentiel en phase de mise en place des procédures et aussi lorsque les objectifs fixés sont progressivement rehaussés pour atteindre le niveau du référentiel à la date souhaitée. Au-delà, il rend compte de l'amélioration continue par ajout de nouveaux items aux objectifs réalisés.

Utilisé en mode témoin de processus pour les items cycliques, l'indicateur alerte le CIL en rétractant à l'avance les sommets concernés du *radar de réalité* en fonction de la périodicité et de la durée estimée de remise en conformité. Idem à l'amorce d'un nouveau traitement.

Il est capable de traduire les variations du référentiel ou des changements intervenant dans le cadre du droit : invalidation *Safe harbor*, prochain règlement européen...

Finalement, cet indicateur est applicable à tout domaine normatif impliquant une *checklist* décomposable en items à vérifier ou réaliser.

6 Conclusion

Le référentiel de gouvernance Informatique et Libertés de la Commission Nationale place le CIL au cœur du pilotage opérationnel des procédures et processus permettant de respecter les principes et droits fondamentaux des personnes.

Ce référentiel établit la liste considérée comme exhaustive des résultats à obtenir mais il est livré sans mode d'emploi détaillé. Pour exploiter son plein potentiel, le CIL doit lui adjoindre un complément méthodologique.

La méthode adoptée afin de transformer ce référentiel en fil conducteur et véritable levier opérationnel se base sur l'identification et le décompte des conditions élémentaires à remplir pour satisfaire les exigences du label. Ces conditions élémentaires isolées – les items – servent en même temps à fabriquer un indicateur de suivi s'adressant à tous les acteurs de la protection des données, leur fournissant en permanence une vision globale de l'essentiel de la gouvernance. Cette vision d'ensemble édiflée dès la phase initiale constitue un facteur primordial d'adhésion à la quête du label.

Ainsi, quatre *vecteurs* de l'espace de gouvernance visualisés sous forme de radars suffisent à répondre aux interrogations récurrentes portant sur la situation réelle d'un établissement vis-à-vis du droit et de ses objectifs mais aussi sur sa capacité à anticiper les changements qui s'annoncent au niveau européen.

Une fois cet indicateur et l'outillage complémentaire dédié à son exploitation mis en place, la démarche consiste à :

1. Positionner sa cible entre le référentiel de la CNIL et les contraintes légales ;
2. Ecrire les procédures à appliquer en vue d'atteindre cette cible et de s'y maintenir ;
3. Mettre en œuvre ces procédures en déroulant les items dans une approche projet.

Bien que les moyens mobilisés soient à adapter aux spécificités locales, l'élaboration des procédures et leur amélioration continue s'effectuent sous la dictée des exigences du label en s'appuyant fortement sur les guides de la CNIL et des réseaux de CIL. La mise en œuvre revient quant à elle à gérer un portefeuille de projets de tailles diverses afin de « réaliser » les items.

La démarche assure l'exhaustivité des actions à engager et, pondérés au besoin par des charges en *jours.homme*, les items calibrent les coûts de la conformité.

Assumé par un CIL se gardant d'accepter une délégation formelle de pouvoir venant du responsable des traitements, le pilotage de toute la gouvernance n'a pas mis en évidence de situation concrète de conflit d'intérêts, invalidant de ce fait la doctrine selon laquelle ce pilotage serait contraire à l'*article 46* du décret d'application d'octobre 2015. En réalité, le terme de pilote est pris ici non pas dans son acception de dirigeant ou de décideur mais dans celles de guide, de conseiller, de vérificateur.

On ne peut finalement éluder que le décompte initial des items du référentiel et la gestion du *radar du droit* nécessitent l'analyse minutieuse de volumineux corpus ainsi qu'une veille de tous les jours. Mais c'est une « constante » de gouvernance qui concerne l'ensemble des établissements et dont la mutualisation profiterait à tous.

Les exigences du label seront en grande partie imposées par le prochain règlement européen et il est nécessaire de préparer la transition.

Gageons que l'intelligence collective ne tardera pas à verser d'autres outils au pot commun.

7 Bibliographie

- [1] CNIL, « Délibération n° 2014-500 du 11 décembre 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et libertés », décembre 2014.
- [2] Conseil UE, « Proposition de règlement du Parlement Européen et du Conseil 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 », juin 2015.
- [3] LIL, « Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », janvier 1978, modifiée 2004.
- [4] DA, « Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », octobre 2005.
- [5] CNIL, « Formulaire de demande de délivrance d'un label pour une procédure de gouvernance Informatique et Libertés », décembre 2014.