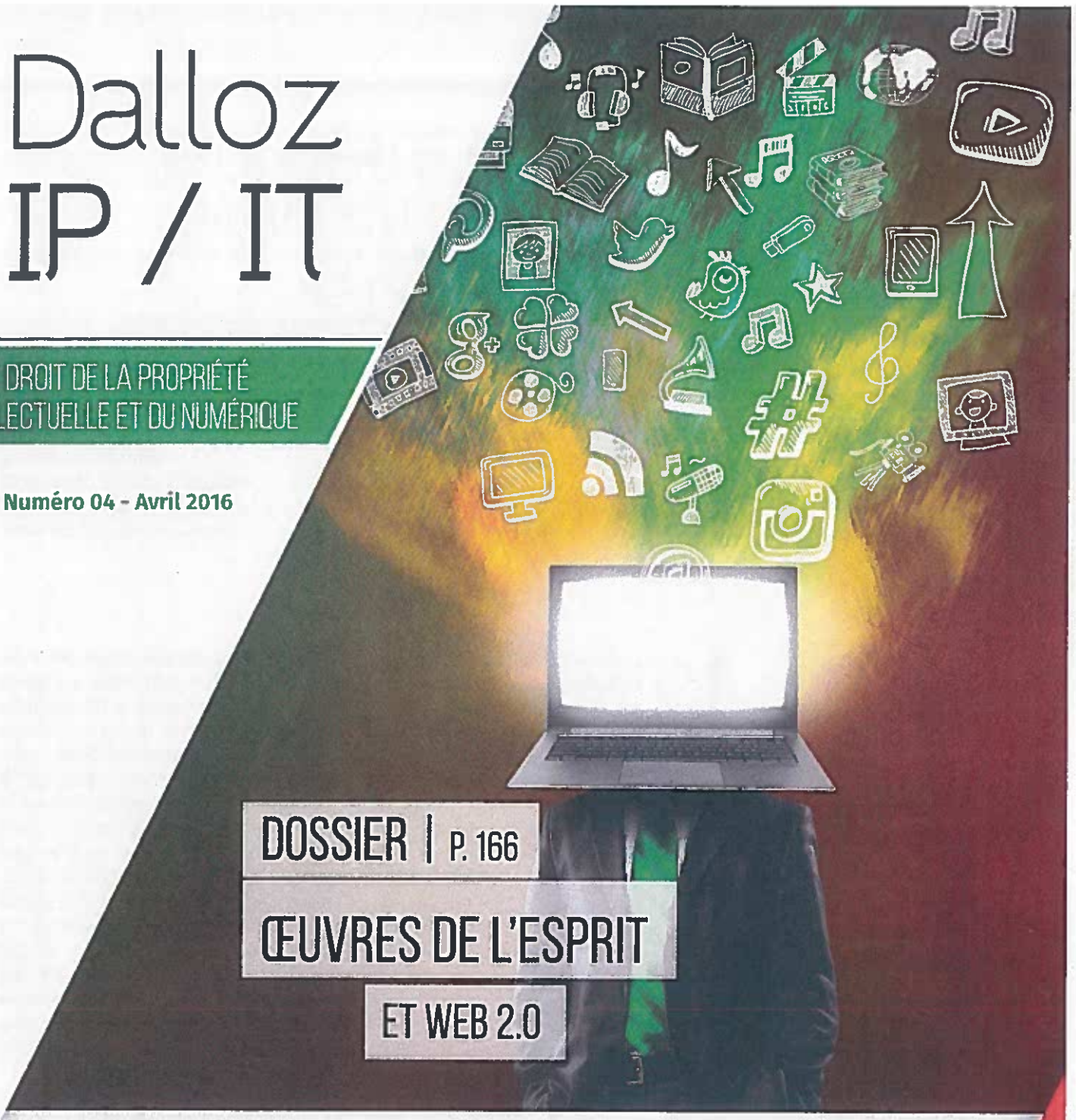
Dalloz IP / IT

DROIT DE LA PROPRIÉTÉ INTELLECTUELLE ET DU NUMÉRIQUE

Numéro 04 - Avril 2016

9 782997 516047



DOSSIER | P. 166

ŒUVRES DE L'ESPRIT ET WEB 2.0

PRATIQUES

L'évolution du rôle du CIL à la lumière du nouveau règlement européen sur les données personnelles

Géraldine Péronne et Emmanuel Daoud

TEXTES ET DÉCISIONS

La mise en œuvre de la jurisprudence européenne sur le lien hypertexte par la Cour d'appel de Paris

Sarah Dormont

TEXTES ET DÉCISIONS

Facebook contre le consommateur français : l'hallali de la clause attributive

Sophie André et Camille Lallemand

DALLOZ

L'ÉVOLUTION DU RÔLE DU CIL À LA LUMIÈRE DU NOUVEAU RÈGLEMENT EUROPÉEN SUR LES DONNÉES PERSONNELLES

Géraldine Péronne
Avocat à la Cour – Cabinet VIGO
(le Cabinet VIGO est membre du réseau GESICA) -
Docteur en droit

Emmanuel Daoud
Avocat à la Cour – Cabinet VIGO
(le Cabinet VIGO est membre du réseau GESICA) -
Membre du Conseil de l'Ordre

Le correspondant informatique et libertés (ci-après « CIL ») a fêté ses dix années d'existence en 2015. Entre les dix ans du CIL et l'entrée en vigueur prochaine du paquet législatif européen dit « Protection des données personnelles », l'heure est au bilan et aux perspectives de cette profession en plein essor.

Instaurée par le décret n° 2005-1309 du 20 octobre 2005 pris en application de la loi Informatique et libertés du 6 janvier 1978[1], la fonction de correspondant informatique et libertés n'a cessé de prendre de l'importance au fil des années[2]. Aujourd'hui, 16 300 organismes en France se sont dotés d'un CIL[3]. Pierre angulaire du paquet européen, le règlement sur la protection des données personnelles vient réformer la loi Informatique et Libertés, déjà modifiée par plusieurs lois successives[4], en renforçant les obligations du responsable de traitement et du sous-traitant. La refonte du rôle du CIL au sein de ce nouvel instrument européen participe de cette évolution. Le législateur européen transforme le correspondant informatique et libertés en *Data Protection Officer* ou DPO. Avant même que le règlement n'entre en vigueur, l'acronyme anglais DPO semble avoir trouvé sa place dans le langage courant et ce, bien plus aisément que le DPD (Délégué à la protection des données). Au-delà du simple changement sémantique, on assiste à une véritable mutation des fonctions de CIL/DPO. Plus que jamais, le règlement dessine les contours d'une culture juridique européenne de la protection des données à caractère personnel, dont le CIL/DPO est la cheville ouvrière.

Le renforcement du rôle du CIL/DPO est indéniable. Cette évolution se traduit en premier lieu, par un renforcement des fonctions (I), et en second lieu, par un renouvellement de ses missions (II).

I - UN RENFORCEMENT DES FONCTIONS

Les fonctions du CIL sont renforcées à trois égards : le règlement rend obligatoire l'exercice de la fonction de CIL dans certaines entreprises ou organisations (A), une expertise spécifique pour exercer cette fonction est requise (B) et l'indépendance du CIL est réaffirmée avec force (C).

1 Loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés. V., N. Metallinos, Maîtriser le risque Informatique et Libertés – La mise en place du correspondant à la protection des données personnelles, Dr. soc. 2006. 378.

2 En atteste la présence de près de 500 personnes, dont majoritairement des CIL à l'Université des correspondants informatique et libertés organisée par l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP) qui s'est tenue le 27 janvier 2016, contre une trentaine, il y a dix ans.

3 https ://www.cnil.fr/fr/cil-un-metier-davenir

4 *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 15 déc. 2015 (OR. En), 15039/15.*

A - Une présence rendue quasi obligatoire

Alors qu'en droit positif la présence d'un CIL dans un organisme est facultative, le règlement européen prévoit une désignation obligatoire dans certains cas :

- premièrement, lorsque le traitement est effectué par une autorité ou un organisme public ;
- deuxièmement, lorsque les activités de base du responsable de traitement consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi particulier et systématique des personnes concernées ;
- troisièmement, lorsque les activités de base du responsable de traitement ou du sous-traitant consistent en des traitements à large échelle, de catégories spéciales de données conformément à l'article 9 et de données relatives à des condamnations ou à des infractions pénales[5].

La dernière version du règlement a fort opportunément écarté le critère du nombre de salariés rendant obligatoire la désignation d'un DPO qui figurait dans la version de 2012 du règlement. La présence d'un CIL était impérative dans l'hypothèse où le traitement était effectué par une entreprise employant 250 personnes ou plus. Or, il existe naturellement de nombreuses petites entreprises traitant des données personnelles en grand nombre. À l'inverse, la masse des ressources humaines d'une organisation n'a pas nécessairement pour corollaire des traitements de données personnelles significatifs. *De facto*, cette nouvelle disposition rend quasiment obligatoire la désignation d'un CIL dans la majorité des organismes, multipliant ainsi le nombre de CIL et favorisant la montée en puissance de la fonction.

B - L'exigence d'une expertise incontestée

La loi Informatique et libertés prévoit que le correspondant est « une personne bénéficiant des qualifications requises pour exercer ses missions »[6]. Le règlement va plus loin puisqu'il énonce que le DPO doit être désigné sur la base de qualités professionnelles, de connaissances expertes du droit des données personnelles et des pratiques et sur la capacité à accomplir les missions prévues à l'article 37[7]. Cette exigence d'une expertise du droit des données personnelles est aujourd'hui essentielle, compte tenu de la complexification de ce droit. On relèvera que le DPO pourra être en relation avec une autorité de contrôle d'un autre pays intervenant en tant que *lead authority*, d'où la nécessité de bien maîtriser le contexte européen dans lequel s'inscrit la protection des données.

Outre la sophistication croissante du droit des données, on assiste également à l'émergence de techniques de collecte et de traitement des données toujours plus complexes et risquées, telles que notamment le *Big Data*, qui supposent d'être bien comprises pour être correctement appréhendées. La transition de la fonction de CIL à la fonction de DPO ne sera pas aisée et supposera donc vraisemblablement des efforts de formation de la part des principaux intéressés. La CNIL aura nécessairement un rôle important à jouer dans la diffusion des connaissances et le partage des expériences.

C - Une indépendance fonctionnelle consolidée

L'article 46 du décret d'application de la loi Informatique et libertés prévoit que le correspondant exerce sa mission directement auprès du responsable de traitement. Le correspondant « ne reçoit aucune instruction pour l'exercice de sa mission »[8]. Cette disposition garantit ainsi l'indépendance du CIL.

L'article 36.3 du règlement prévoit quant à lui que le DPO doit faire directement rapport au niveau de management le plus élevé du responsable de traitement ou du sous-traitant. Il ne s'agit plus pour le CIL d'exercer ses missions auprès du responsable de traitement, mais de faire rapport de son activité et d'être rattaché

5 Art. 35 du règlement version 2015.

6 Art. 22 III de la loi n° 78-17 du 6 janv. 1978.

7 Art. 35.5 du règlement.

8 Art. 46 du décr. n° 2005-1309 du 20 oct. 2005.

au niveau le plus élevé de la hiérarchie au sein de l'organigramme.

On place ainsi le DPO au plus près de la direction générale, de manière à garantir son indépendance, mais aussi à envoyer un message fort : le DPO occupe une place importante dans l'organisme.

Cette indépendance fonctionnelle renforcée se double d'une prise de conscience très claire des enjeux du métier de DPO, puisqu'il est expressément prévu dans le règlement qu'il sera lié par une obligation de secret et de confidentialité au regard de ses activités, ce qui paraît tout à fait indispensable compte tenu des données sensibles dont il peut avoir connaissance[9]. L'indépendance du CIL paraît encore favorisée par la suppression dans le règlement de la condition de seuil pour nommer un CIL externe. En effet, le décret du 20 octobre 2005 prévoyait que lorsque plus de cinquante personnes étaient chargées de la mise en œuvre ou avaient directement accès aux traitements de données, le responsable de traitement devait désigner un CIL exclusivement attaché au service de la personne morale, organisme ou autorité publique[10]. L'article 35.8 du règlement ne reprend pas cette exigence de seuil et rend possible la désignation d'un DPO salarié ou d'un DPO lié par un contrat de service, donc un DPO externe, sans autre condition. Cette disposition ouvre de nouvelles perspectives à la profession d'avocat CIL, activité autorisée depuis 2009 et qui a ainsi vocation à s'épanouir sans entraves[11].

Ces observations conduisent à un constat qui est déjà largement partagé par les CIL en exercice, il sera de plus en plus difficile de concilier la fonction de CIL avec l'exercice d'une autre fonction au sein de l'organisme, comme c'est souvent le cas. DPO, un métier à temps plein ? Cette question se pose avec encore plus d'acuité au regard des nouvelles missions qui incombent au DPO en vertu du texte européen.

PERSPECTIVES

Si le DPO devient une figure incontournable de la protection des données à l'aune du règlement, le texte fait également naître de nouvelles questions. Le DPO peut-il concilier cette fonction avec une autre fonction au sein de l'organisme ? Comment former au mieux les DPO pour qu'ils puissent exercer leurs missions sereinement ? Peut-être manque-t-il à présent à ce nouvel édifice un ensemble de règles qui préciseraient les obligations éthiques du DPO et façonneraient l'unité d'une profession dont les profils sont souvent variés. À quand un code de déontologie du DPO ?

II - UN RENOUVELLEMENT DES MISSIONS

Le renforcement des fonctions et partant, du statut du DPO au sein de l'organisme pour lequel il travaille, a pour corollaire un renouvellement des missions assignées au DPO. Ce dernier se doit de veiller à la bonne application du règlement (A), d'être l'artisan des études d'impact sur la vie privée (B) et d'être un point de contact avec l'autorité de contrôle (C).

A - Le DPO, garant de la bonne application du règlement

En vertu du nouveau règlement et conformément à ce qui était déjà prévu par la loi Informatique et libertés, le CIL/DPO conseille et informe le responsable de traitement[12].

Le règlement innove, en revanche, lorsqu'il assigne au DPO la mission de contrôler l'application du règlement[13]. Il ne s'agit plus seulement pour le CIL d'informer le responsable de traitement en cas de manquements[14], mais de se placer en garant de la conformité des actions entreprises au sein de l'organisme. Le texte précise qu'il s'agit de s'assurer de la bonne répartition des responsabilités, de la sensibilisation du personnel, de la formation et des audits. Cette disposition, dont la clarté n'est pas la caractéristique principale, pourrait être interprétée comme faisant naître une responsabilité du CIL en cas de violation des dispositions du règlement. Cette interprétation serait toutefois inadéquate. En effet, il ne peut y avoir de transfert de responsabilité du responsable de traitement vers le DPO en cas

9 Art. 36.4 du règlement.

10 Art. 44 du décr. n° 2005-1309 du 20 oct. 2005.

11 Art. 6.2.2 du règlement intérieur national de la profession d'avocat.

12 Art. 49 du décr. n° 2005-1309 du 20 oct. 2005.

13 Art. 37 b) du règlement.

14 Art. 49 du décr. n° 2005-1309 du 20 oct. 2005.

de manquement avéré. Le responsable de traitement reste responsable de toute violation des dispositions du règlement, comme l'indiquent clairement les articles 5, 22 et 24 du règlement [15].

B - Le DPO, artisan des études d'impact sur la vie privée

Le règlement européen impose au DPO de prodiguer au responsable de traitement des conseils sur l'analyse d'impact et de surveiller son application [16]. Il y a fort à parier que sa mission ira au-delà des simples conseils et qu'il sera en réalité l'artisan de ces études, tant son expertise du droit des données personnelles le promet à cette nouvelle mission. Le règlement rend l'étude d'impact obligatoire dans l'hypothèse d'un traitement de données qui comporterait un risque élevé d'atteinte aux droits et libertés des individus. Cette étude d'impact doit comporter un certain nombre d'informations et notamment une description systématique du traitement envisagé, une étude de la nécessité et de la proportionnalité du traitement, une étude des risques pour les droits et libertés des personnes concernées et les mesures envisagées pour couvrir ces risques [17].

La CNIL a devancé les attentes et mis à la disposition des CIL/DPO deux guides très détaillés sur la manière de mener une étude d'impact [18]. La longueur de ces documents est révélatrice de la complexité de la tâche à accomplir et de la charge de travail importante qui va incomber au DPO.

C - Le DPO, point de contact privilégié avec l'autorité de contrôle

Deux missions incombant au DPO à l'aune du texte européen nécessitent encore une attention particulière. Le règlement instaure deux nouvelles obligations. La première consiste à notifier à l'autorité de contrôle compétente une faille de sécurité dans les 72 heures, sous certaines conditions [19]. La seconde consiste à communiquer sans délai l'existence de cette faille aux personnes concernées [20]. Le DPO est amené à jouer un rôle essentiel dans ces deux cas.

Premièrement, la notification à l'autorité de contrôle doit comporter une communication à cette dernière des coordonnées du DPO. La notification doit ensuite comprendre une documentation relative à la nature du dysfonctionnement, le nombre de personnes concernées, les données visées, les mesures prises ou envisagées pour pallier cette faille, etc. On comprend aisément que le DPO sera le point de contact privilégié entre l'organisme victime d'une faille de sécurité et l'autorité de contrôle.

Deuxièmement, la communication de la faille de sécurité aux personnes concernées suppose encore une fois que les coordonnées du DPO fassent partie des informations transmises à la personne concernée [21], de sorte que le DPO sera en première ligne pour répondre aux réclamations et interrogations des personnes concernées par la faille de sécurité.

Le DPO jouera donc un rôle de relais entre les personnes victimes et l'organisme.

Point de contact, personne relais, personne ressource, les qualificatifs ne manquent pas pour redéfinir les missions du DPO, qui voit ses fonctions dépasser le simple cadre de l'organisme pour lequel il travaille. Si cette ouverture n'est pas en elle-même nouvelle, le CIL n'ayant jamais été un travailleur isolé, elle prend une nouvelle dimension car le DPO devient un véritable représentant de l'organisme.

Cela implique d'une part, une coopération très étroite entre le responsable de traitement et le DPO afin de définir les conditions dans lesquelles seront communiquées les informations relatives aux failles de sécurité à l'autorité de contrôle et aux personnes concernées. Le DPO se devra, d'autre part, d'être un excellent communiquant, de manière à limiter les risques d'atteinte à la réputation découlant de la révélation de ces failles.

■ 15 En ce sens, on relèvera que le principe *d'accountability* fait son entrée dans le règlement et implique que le responsable de traitement rende compte de ses activités et réponde de ses actes, notamment auprès de l'autorité de contrôle. V., R. Gola, La proposition de règlement européen sur les données personnelles, enjeux et opportunités pour l'entreprise et les citoyens, RLDI 2015. 121. V. égal. W. Maxwell et S. Taieb, *L'accountability*, symbole d'une influence américaine sur le règlement européen des données personnelles ?, Dalloz IP/IT 2016. 123.

■ 16 Art. 37, b) du règlement.

■ 17 Art. 33 du règlement.

■ 18 *Étude d'impact sur la vie privée (EIVP) Privacy Impact Assessment – Comment mener une étude d'impact*, CNIL, éd. juin 2015 ; *ibid.*, – *Modèles et bases de connaissances*.

■ 19 Art. 31 du règlement.

■ 20 Art. 32 du règlement.

■ 21 Art. 32.2 du règlement.