L'*ACCOUNTABILITY*, SYMBOLE D'UNE INFLUENCE AMÉRICAINE SUR LE RÈGLEMENT EUROPÉEN DES DONNÉES PERSONNELLES ?

*Après avoir retracé les origines et les différents aspects que recouvre ce terme, les auteurs replacent l'*accountability *dans l'univers des données personnelles. Ils mettent en perspective l'*accountability *lorsqu'elle est au service de la protection de ces données, à la fois comme outil de co-régulation, à travers le label CNIL « Gouvernance Informatique et Libertés » et dans la référence faîte à cette notion par le futur règlement européen. C'est enfin à une ultime approche prospective que les auteurs se livrent.*

Winston Maxwell
Avocat, Hogan Lovells (Paris)

et Sarah Taïeb
Avocat, Hogan Lovells (Paris)

Avant d'être utilisé dans le contexte de la protection des données à caractère personnel, le terme « *accountability* » se référait principalement à l'obligation des mandataires de rendre compte à leurs mandants. Dans le cadre des institutions publiques, les élus doivent rendre compte à leurs électeurs, le Gouvernement doit rendre compte au Parlement et aux citoyens. En matière de droit des sociétés, les mandataires sociaux doivent rendre compte aux actionnaires. En droit américain, les mandataires sociaux ont un devoir fiduciaire (*fiduciary duty*) qui les oblige à placer les intérêts de la société et de ses actionnaires avant leurs propres intérêts et *démontrer* aux actionnaires qu'ils ont agi dans le seul intérêt de la société.

Lorsque l'on parle d'*accountability* dans le contexte de la protection des données à caractère personnel, on pense souvent aux systèmes de gouvernance de la conformité mis en œuvre au sein de groupes multinationaux. Ces systèmes se sont généralisés à la suite d'un décret adopté par le Gouvernement américain en 1991 concernant l'application de sanctions financières à l'égard d'entreprises privées[1]. Ce décret prévoit que les entreprises ayant mis en place un système de gouvernance de la conformité bénéficieront d'une réduction des amendes applicables par rapport aux entreprises n'ayant pas adopté un tel système. Le décret vise la conformité au sens large : lois sur l'environne-

[1] *US Sentencing Commission Guidelines, Sentencing for Organizations*, 56 Fed. Reg. 22,762 (1991), telle que modifiée avec effet au 1er nov. 2004, Fed. Reg. 28,994-29,028 (19 mai 2004).

ment, comptabilité, délits boursiers, corruption, concurrence... L'entreprise doit mettre en place des procédures internes pour prévenir et détecter des actes illégaux commis par les salariés, organiser des séances de formation et des audits. L'entreprise doit avoir un directeur de la conformité (*Chief Compliance Officer* [CCO]), responsable de la mise en place du système de conformité. Le CCO doit disposer de ressources adéquates pour assurer sa fonction et rendre compte directement au conseil d'administration.

Le terme Accountability *est généralement traduit par responsabilisation*

Suite à la faillite d'Enron, les contraintes en matière de conformité ont été renforcées avec l'adoption de la loi Sarbanes-Oxley[2]. La législation américaine sur la conformité a encore été renforcée après la faillite de la banque Lehman Brothers avec l'adoption du « *Dodd-Frank Act* »[3]. Ces lois imposent notamment l'obligation de disposer de systèmes permettant à des lanceurs d'alertes de remonter des informations concernant d'éventuelles infractions vers le comité d'audit et le CCO, en contournant les voies hiérarchiques classiques. Le CCO a uniquement un devoir envers le conseil d'administration. Il n'a pas un devoir, tel un commissaire aux comptes, de dénoncer lui-même des infractions auprès des autorités. La décision de s'auto-dénoncer revient uniquement à la direction de l'entreprise.

Un autre aspect important de l'*accountability* est la délégation par le régulateur de certains pouvoirs normatifs. Cette délégation s'est faite en matière de droit de l'environnement et devient fréquente en matière de protection de données à caractère personnel. On parle de « co-régulation ». Dans une approche d'*accountability*, cette délégation s'accompagne du devoir de rendre compte de la bonne exécution de la mission. Cela signifie que l'entreprise doit disposer d'une structure de gouvernance pour assurer la qualité de la norme qu'elle crée. Des contrôles internes seront nécessaires pour assurer que la norme développée au sein de l'entreprise tient compte des objectifs du régulateur. Certaines démarches seront nécessaires en interne (études d'impact...) pour établir la norme et pouvoir démontrer qu'elle a été adoptée dans de bonnes conditions. On essaiera d'appliquer au sein de l'entreprise les mêmes démarches qu'un régulateur aurait appliquées si le régulateur avait élaboré la norme. On imite la fonction de régulation, en le déplaçant à l'intérieur de l'entreprise.

I - L'*ACCOUNTABILITY* AU SERVICE DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Dans le monde des données personnelles, le terme *accountability* est généralement traduit par « responsabilisation ». Il s'agit pour l'organisme de « mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données »[4].

La notion d'*accountability* dans les textes. De nombreux textes ont, depuis 1980, fait référence à la notion d'*accountability* dans le domaine de la protection des données personnelles.

L'OCDE fut pionnière en la matière avec ses Lignes directrices de 1980[5] régissant la protection de la vie privée incluant un paragraphe intitulé « *Accountability principle* ». L'OCDE affirmait la responsabilité du maître de fichier quant au respect des mesures donnant effet aux principes des Lignes directrices. Une norme ISO de 2011 relative à la vie privée[6] inclut également une section intitulée « *Accountability* ». L'*accountability* est, selon l'ISO, une obligation de diligence (*duty of care*) à laquelle s'ajoute l'adoption de mesures concrètes et pratiques assurant la protection des données. Au niveau européen, la directive 95/46/CE relative aux données personnelles[7] ne fait pas spécifiquement référence au terme *accountability* mais certaines de ses dispositions impliquent

2 Sarbanes Oxley Act (SOX) 18 USC §1514A.

3 Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, 124 Stat. 1376 (2010).

4 CNIL, Rapport d'activité 2014, p. 89.

5 Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, OCDE, 1980, révisées en 2013.

6 ISO/IEC 29100 :2011, Information technology - Security techniques - Privacy framework.

7 Dir. 95/46/CE du Parlement européen et du Conseil du 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

cette notion, et notamment l'obligation de mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données. L'avis du Groupe de l'Article 29 « *On the principle of accountability* » a défini l'*accountability* comme mettant « l'accent sur la manière dont la responsabilité (*responsability*) est assumée et sur la manière de le vérifier »[8].

L'*accountability* comme outil de co-régulation. Le cadre APEC pour la protection des données personnelles[9], la politique de protection des données personnelles de la Maison Blanche dans le cadre de l'*US Consumer Bill of Rights*[10] et les nouvelles recommandations de l'OCDE de 2013 ont accordé une importance plus particulière au concept d'*accountability*. Ces textes font de l'*accountability* une forme de co-régulation entre les responsables de traitement et les autorités, consistant en la mise en place de programmes de conformité à l'intérieur des entreprises et de la supervision de ces mesures par les autorités de l'État.

Un exemple type de co-régulation est l'adoption de *Binding Corporate Rules* (BCR). Les BCR désignent un code de conduite interne qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne. L'adoption de BCR permet notamment d'être en conformité avec les principes de la directive 95/46/CE, de communiquer sur la politique d'entreprise en matière de protection des données personnelles et d'assurer un niveau de protection satisfaisant lors des transferts de données personnelles[11]. On retrouve ici deux ingrédients essentiels de l'*accountability* : la conformité et la transparence.

Le label CNIL « Gouvernance Informatique et Libertés ». En 2015, la Commission nationale de l'informatique et des libertés, la CNIL, a publié un « référentiel gouvernance »[12]. Le référentiel est divisé en vingt-cinq exigences relatives à l'existence de politiques de protection des données personnelles ainsi qu'à la désignation d'un Correspondant informatique et libertés (CIL), l'équivalent français du *Data Protection Officer* (DPO).

Les organismes démontrant qu'ils se conforment au nouveau référentiel pourront obtenir de la CNIL un « label Gouvernance Informatique et Libertés ». L'obtention d'un label CNIL permet notamment de : (i) « se distinguer en garantissant un haut niveau de protection des données personnelles », (ii) « afficher un indicateur de confiance » et (iii) « renforcer la crédibilité » de l'organisme[13]. L'obtention du « label Gouvernance Informatique et Libertés » se présente dès lors, à ce jour, comme étant le *nec plus ultra* de l'*accountability* en France.

La désignation d'un CIL est au cœur du label et sa fonction très encadrée. Le référentiel exige que la fonction de CIL soit rattachée à un membre de l'instance exécutive. Le CIL doit bénéficier d'une formation continue. Un budget et des moyens propres doivent lui être alloués. Le CIL est consulté sur tous les projets impliquant des traitements de données. Il est également responsable de la réalisation d'actions de sensibilisation en interne. Le CIL doit procéder à une analyse juridique des traitements opérés, élaborer des recommandations et proposer un plan d'action de prévention et de correction lorsque nécessaire. Il doit s'assurer qu'une analyse des risques a bien été effectuée. Le référentiel renforce le rôle du CIL, qui se rapproche du rôle du "*Chief Compliance Officer*" dans les systèmes de gouvernance américain, et du rôle du DPO envisagé par le nouveau règlement européen.

Le règlement européen en matière de protection des données à caractère personnel (le « Règlement »)[14]. L'accord trouvé le 15 décembre 2015 par le comité LIBE du Parlement européen, le COREPER et la Commission européenne sur la réforme européenne de la protection des données marque l'une des dernières étapes vers l'adoption finale du Règlement. Le texte final fait spécifiquement référence à l'*accountability*. La notion est introduite à l'article 5 comme suit : « *The*

8 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf

9 *Asia-Pacific Economic Cooperation (APEC) Privacy Framework*, disponible sur http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

10 *United States White House, « Consumer data privacy in a networked world : a framework for protecting privacy and promoting innovation in the global digital economy »*, févr. 2012.

11 Guide de la CNIL « Tout savoir sur les BCR » http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/CNIL-transferts-BCR.pdf

12 Délib. n° 2014-500 du 11 déc. 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et Libertés, disponible sur http://www.legifrance.gouv.fr/jo_pdf.do ?cidTexte=JORFTEXT000030073950.

13 CNIL, Rapport d'activité 2014, p. 43.

14 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) [first reading] - Analysis of the final compromise text with a view to agreement, 15039/15, 15 déc. 2015.

PERSPECTIVES

Les labels *accountability*. La pratique d'*accountability* en Europe dépendra en grande partie des normes établies par les autorités de régulation nationales dans le cadre de certifications, mentionnées à l'article 39 du Règlement. Ces mécanismes de certification seront établis soit au niveau national, ou au niveau de l'Union. La CNIL est précurseur car elle a d'ores et déjà établi un label qu'elle peut accorder à des organismes qui mettent en œuvre des programmes d'*accountability* répondant aux critères de gouvernance qu'elle a établis. Le référentiel CNIL incorpore déjà les éléments clés d'*accountabililty* exigés par le Règlement, et pourrait servir de modèle pour le développement d'une future certification européenne.

controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability") ». Le paragraphe 1 en question liste six principes généraux relatifs au traitement des données. L'*accountability*, au sens du Règlement, serait donc une situation dans laquelle l'entreprise serait capable de démontrer qu'elle agit en conformité avec les principes du Règlement.

*On assiste à une transformation de l'*accountability

L'article 22, intitulé « *Responsibility* », réitère l'obligation de *démontrer* la conformité. Cela passe par la mise en place de mesures techniques et d'organisation appropriées, la mise en place de politiques de protection des données personnelles, l'adhésion à des codes de conduite approuvés, mécanisme de certification agréé.

Le DPO. La section IV du Règlement est dédiée au DPO. La désignation d'un DPO n'est obligatoire que dans certains cas et notamment lorsque des données sensibles font l'objet d'un traitement. Le DPO est choisi pour son expertise et rend compte au niveau de direction le plus élevé de l'entreprise. Le DPO devient un acteur stratégique de l'entreprise, à l'instar du *Chief Compliance Officer*. Il doit être impliqué dans toutes les problématiques impliquant des traitements de données, et veiller à la mise en œuvre des politiques de protection des données personnelles au sein de l'entreprise, notamment en organisant des formations et un réseau de personnes sensibilisées aux problèmes de données personnelles dans l'entreprise. Le DPO veille à la mise en place d'audits, et contribue à l'élaboration d'études d'impact. Il doit disposer des ressources et informations nécessaires pour effectuer ces taches et des moyens de bénéficier d'une formation continue. Il est un point de contact pour les autorités de contrôle, et devra coopérer avec elles. Le DPO informe, conseille et contrôle la bonne application des principes du Règlement. Par exemple, concernant les audits, le DPO a seulement pour rôle de contrôler la mise en place d'audits, non de les réaliser lui-même. Lorsque l'audit est réalisé par un tiers indépendant et neutre, plutôt que par le DPO lui-même, cela contribue à l'indépendance du DPO. Le rôle de DPO ressemble au rôle de CCO décrit dans le décret américain de 1991 et le rôle de CIL renforcé décrit dans le référentiel CNIL de 2015.

Impact de l'*accountability* sur les sanctions potentielles. Le Règlement va augmenter le niveau des sanctions administratives, qui pourront atteindre 4 % du chiffre d'affaires global du groupe. Le niveau de sanctions devra tenir compte des mesures prises par le responsable de traitement afin d'assurer la conformité (mesures techniques et d'organisation prises pour prévenir ou réduire le dommage, niveau de coopération avec l'autorité de contrôle, mise en application par l'entreprise de codes de conduite ou de procédés de certification). Même si le Règlement est moins explicite que le décret américain de 1991, on comprend que la mise en œuvre de l'*accountability* devrait réduire le montant des amendes potentielles.

II - QUEL FUTUR POUR L'*ACCOUNTABILITY* ?

Depuis 2013 et la révision des Lignes directrices de l'OCDE, on assiste à une transformation de l'*accountability* qui va beaucoup plus loin que la simple mise en place de mesures permettant la conformité. L'*accountability* est devenue un prin-

cipe clé dans le domaine de la protection des données personnelles. L'*accountability* d'aujourd'hui, post-adoption du Règlement, est un prisme à trois facettes.

La première facette est l'établissement par l'entreprise d'une norme « sur-mesure », qui définit un cadre à respecter prenant en compte le plus possible le contexte, les activités et les contraintes inhérentes à l'entreprise concernée. Les différentes autorités peuvent accompagner les entreprises dans la création de ce cadre normatif. La CNIL, par exemple, a récemment mis en place des « packs de conformité » par secteur professionnel (comme le pack Assurance) que la CNIL définit comme étant des « outils de pilotage de la conformité pour les secteurs professionnels qui en bénéficient »[15]. On assiste ici à une décentralisation du pouvoir normatif. L'entreprise se substitue en quelque sorte au régulateur pour la mise au point de règles internes.

La deuxième facette consiste à rendre l'application des normes efficace et vérifiable. Cela passe par la formation des personnes, un mécanisme d'incitation des salariés d'adopter une « culture de conformité », ainsi qu'un mécanisme de détection de la non-conformité par le biais d'audits, d'enquêtes internes, de systèmes d'alerte, comme les alertes professionnelles ou *whistleblowing*. Un système de gouvernance est nécessaire pour éviter les conflits d'intérêts et l'inefficacité du cadre normatif. C'est là qu'intervient le DPO, agent clé de l'*accountability*. Rendant compte à l'organe de direction le plus élevé de l'entreprise, le DPO dispose d'une indépendance par rapport aux différents départements opérationnels de l'entreprise.

La troisième facette permet une sorte d'exploitation commerciale des deux autres. Elle consiste en un système de transparence permettant la transmission de l'image et des valeurs de l'entreprise au monde extérieur afin de gagner ou regagner la confiance du public et du régulateur. Comme mentionné par le Groupe de l'Article 29, « on ne peut inspirer une confiance suffisante que s'il est démontré que la responsabilité (*responsability*) est efficacement assumée dans la pratique ». La protection des données personnelles est devenue, en grande partie, définie par ce qu'attendent les clients de l'entreprise concernant le traitement de leurs données[16]. La conformité et sa démonstration sont un moyen d'affirmer son attachement à la protection des données personnelles et est devenu « un enjeu de crédibilité »[17].

Le DPO, agent clé de l'accountability

DOSSIER

15 http://www.cnil.fr/linstitution/actualite/article/article/les-packs-de-conformite-un-succes-grandissant/

16 Privacy on the books and on the ground, Kenneth A. Bamberger & Deirdre K. Mulligan.

17 CNIL, Rapport d'activité 2014, p. 42.