cigref
Réseau
de Grandes Entreprises

PROMOUVOIR LA CULTURE NUMERIQUE
COMME SOURCE D'INNOVATION ET DE PERFORMANCE

Éthique et Numérique

Enjeux et recommandations à l'intention des entreprises

Juillet 2014

SYNTHÈSE

Le caractère omniprésent du numérique dans nos sociétés et nos entreprises et les transformations profondes qui en découlent, tant au niveau sociétal qu'économique, témoignent d'un nouveau paradigme technologique. Ce nouveau paradigme suppose par conséquent la (re)définition de valeurs sociales et éthiques. Avec l'évolution des potentialités technologiques, de nombreuses opportunités se créent pour le monde économique en même temps que de nouveaux risques éthiques. La rédaction de ce rapport a été motivée par trois constats majeurs :

- **L'éthique, un complément essentiel au respect du cadre règlementaire**

L'éthique concerne un autre champ d'application que celui de la juridiction ou des règles de sécurité. L'éthique suggère non pas l'obéissance aveugle à un ensemble de règles quelconques, mais plutôt l'autorégulation, l'implication, la responsabilisation des individus autour de certaines normes intangibles comme la loi ou de certaines valeurs promues par l'entreprise. L'enjeu de l'éthique, étymologiquement « étude des comportements » (*ethos*) est de créer un sentiment de responsabilité à tous les niveaux de la hiérarchie et de la chaîne de création de valeur, non seulement en respectant le cadre réglementaire, mais aussi et surtout en définissant soi-même ses propres règles, principes ou limites (en fonction des possibilités qui s'offrent à nous ou de la nature interprétative d'une loi, etc.).

- **La confiance, un élément de différenciation concurrentielle**

Plusieurs études — *Future of Digital Trust*, réalisée par Orange ; la 3ème vague du Baromètre *La confiance des Français dans le numérique*, réalisée par l'IDATE (Institut De l'Audiovisuel et des Télécommunications en Europe) — signalent un fait marquant : la confiance des clients/consommateurs est aujourd'hui en crise. Plus de trois quarts des clients/ consommateurs se révèlent être méfiants vis-à-vis de la gestion et de l'utilisation de leurs données personnelles par les entreprises. Préserver la confiance des clients autour d'une transparence, d'une pédagogie, d'une honnêteté sur la finalité des traitements des données devient une préoccupation majeure.
La pérennité du succès de l'entreprise numérique repose aujourd'hui, plus que jamais, sur la capacité à co-construire un socle de confiance partagée dans toute « l'entreprise étendue », et à prendre en compte l'acceptabilité sociale. Cette démarche est sans conteste la marque d'une différenciation concurrentielle, valorisante pour l'entreprise.

- **Adapter les recommandations au contexte numérique des entreprises**

Ce rapport apporte un éclairage sur les problématiques éthiques qui se posent aujourd'hui dans le cadre de la transformation numérique des entreprises. Plusieurs enjeux ont été répertoriés et analysés afin de poser un cadre général à la

compréhension du sujet : l'infobésité, le droit à la déconnexion, le droit à l'oubli, la dématérialisation des liens sociaux, le traitement des données personnelles. Un guide méthodologique et pratique ainsi qu'une grille de recommandations ont été élaborés dans le but de faciliter la prise en compte de ces nouveaux enjeux dans la définition de règles éthiques, dans toute l'entreprise étendue.

Faire une éthique du numérique suppose la prise en compte d'une nouvelle chaîne de responsabilités qui concerne à la fois les concepteurs et programmeurs / les dirigeants, managers et décideurs / et les utilisateurs finaux.

Le CIGREF, réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de promouvoir la culture numérique comme source d'innovation et de performance.

Titre du rapport : *Éthique et Numérique : Enjeux et recommandations à l'intention des entreprises*

Equipe du CIGREF

Jean-François PÉPIN – Délégué général
Sophie BOUTEILLER – Directrice de mission
Anne-Sophie BOISARD – Directrice de mission
Josette WATRINEL – Secrétaire de direction
Flora FISCHER – Assistante de mission
Frédéric LAU – Directeur de mission
Matthieu BOUTIN – Chargé de mission
Marie-Pierre LACROIX – Chef de projet
Josette LEMAN – Assistante de direction

REMERCIEMENTS :

Le groupe de travail « *Ethique et Numérique* » a été piloté par **Georges EPINETTE, DOSI du Groupement des Mousquetaires et Vice Président du CIGREF**, et animé par **Sophie BOUTEILLER et Flora FISCHER**

Nous remercions sincèrement les personnes qui ont participé aux échanges :

Sophie ALLAIRE	Total	Isabelle GOHIN-DUFOUR	Allianz Informatique
Jacques BOURDOS	Renault	Pascal HERVIER	Bolloré
Frédéric CERBELAUD	SNCF	Chloé KLENIEC	SNCF
Philippe CROSNIER	BPCE	Marie-Christine LACLAUTRE	Allianz Informatique
Sophie DELMAS	BNP Paribas	Yann-Maël LARHER	Total
Mahmoud DENFER	Vallourec	Pascal LEON	PSA
Véronique DURAND-CHARLOT	GDF Suez	Catherine PONS	GMF
Michelle FORT	SNCF	François SUBRENAT	ONF
Marie-Noëlle GIBON	La Poste		

Ce rapport a été rédigé par Flora FISCHER, Assistante de mission.

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER LE CIGREF AUX COORDONNÉES CI-DESSOUS :

CIGREF, Réseau de Grandes entreprises
21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00
Courriel : contact@cigref.fr

Sites internet :
http://www.cigref.fr/
http://www.fondation-cigref.org/
http://www.histoire-cigref.org/
http://www.questionner-le-numerique.org
http://www.entreprises-et-cultures-numeriques.org

TABLE DES MATIÈRES

Introduction

Depuis 2006, le CIGREF mène une réflexion sur la déontologie liée aux usages des systèmes d'information. L'importance de ce thème est aujourd'hui renforcée par l'omniprésence du numérique. Il introduit une transformation profonde dans les entreprises, un changement de paradigme qui intervient tant sur l'organisation et les modes de management que sur les relations humaines. La nature du travail change et les frontières de l'entreprise s'étendent. Cette transformation introduit à la fois de nouvelles opportunités pour l'économie et de nouvelles problématiques éthiques associées. Chaque acteur de l'entreprise doit être invité à maîtriser les potentialités des nouveaux outils et usages du numériques en même temps que leurs possibles déviances.

L'objectif du groupe de travail "Éthique et numérique" était d'aboutir à une compréhension plus précise des enjeux éthiques spécifiques au numérique dans le contexte de l'entreprise, en commençant par **qualifier les enjeux éthiques** émergents et en ouvrant une **réflexion sur leurs impacts** pour l'entreprise et la société.

Il ne s'agit pas de proposer une boîte à outils ou un « prêt à penser » destinés à livrer des modèles d'actions pour parer les risques éthiques :

- d'une part parce que **les problématiques éthiques sont spécifiques à la nature de chaque entreprise et ne sauraient être universalisées à l'ensemble du monde entrepreneurial**,
- d'autre part, parce que **l'éthique est une démarche réflexive, un questionnement, une recherche, qui ne donne pas de réponses certaines et univoques à une question.** Nous parlons d'éthique parce que nous nous posons des questions auxquelles nous ne savons pas (encore) répondre. C'est ce qui différencie l'éthique du juridique. Le droit permet de régler et de sanctionner au travers de juridictions préétablies et s'applique indifféremment de l'appréciation de chacun. L'éthique en revanche n'a de sens et de valeur que si chaque individu se l'approprie. Elle ne vise pas une régulation universelle mais plutôt une autorégulation (que chaque individu ou chaque collectif s'applique à lui-même).

1. Les enjeux éthiques dans la transformation numérique de l'entreprise

Plusieurs thématiques ont été traitées et analysés par le groupe de travail : elles sont représentatives des principaux enjeux éthiques que pose l'usage du numérique en entreprise.

1.1. Infobésité

L'infobésité, ou surcharge informationnelle et cognitive, impacte tant la productivité du salarié que sa sociabilité et sa santé mentale. Le rapport CIGREF *Usage des TIC et RSE* (2009) observe en effet, d'une part que « *l'hypertrophie des flux de données a une conséquence immédiate sur les proportions de temps passé à la lecture et au traitement des données* »[1]. Ainsi, le temps passé à traiter des données capte une énergie précieuse et conduit de plus au renforcement de l'individualisation du travail : **« *nous entrons dans une situation paradoxale où les communications interpersonnelles produisent de l'isolement* »[2].** D'autre part, une étude de 2007 portée par des chercheurs britanniques[3], Karen Renaud, informaticienne de l'Université de Glasgow et Judith Ramsay, psychologue, montre que **plus d'un salarié sur trois souffre de stress en raison de l'avalanche de mails qu'il reçoit sur son lieu de travail.**

1.2. Droit à la déconnexion

La vitesse et la démultiplication des capacités de stockage des données rendent possible **un usage abusif des emails, ce qui, dans le cadre professionnel, occasionne une connectivité ininterrompue favorisant le brouillage des frontières entre vie privée et vie professionnelle**, et

[1] *Usage des TIC et RSE*, rapport CIGREF, 2009, p.21

[2] Ibid

[3] Article sur l'étude : http://www.generation-nt.com/stress-email-messagerie-travail-actualite-43990.html

une réactivité presque instantanée. L'employé peut devenir improductif si son temps de travail est sans cesse interrompu et fragmenté par le flux d'informations qui circule sur les réseaux et les boîtes mails. Il a fallu de nombreuses années pour se rendre compte que l'usage intempestif des mails occasionne des conséquences non négligeables sur le bien-être et la productivité au travail : ce n'est que depuis les années 2000 que l'on parle d'instituer un droit à la déconnexion. A titre d'exemple, certaines entreprises ont aujourd'hui mis en place des règles drastiques, en amont de la loi, afin de garantir le droit à la déconnexion, comme Volkswagen qui a décidé d'arrêter d'envoyer des mails sur les *Blackberry* de ses cadres, en dehors des horaires de travail.

1.3. Dématérialisation des objets et des liens sociaux

L'organisation en équipe virtuelle, la distanciation et l'immatérialité du travail engendrent un sentiment de perte de contrôle pour le management intermédiaire.

Pourtant, paradoxalement, « l*es TIC sont dotées de capacités informationnelles et de capacités de surveillance essentielles au processus de contrôle* »[4].

Les procédés de contrôle immatériels se révèlent être parfois plus puissants que les procédés traditionnels. Ils peuvent alors causer plus de pression chez les employés lorsqu'ils sont soumis à une surveillance électronique par exemple : « [Les TIC] *rendent le travail plus visible et sont de fait susceptibles d'affecter la capacité de contrôle du manager, et, plus largement la relation managériale*. *En outre la capacité de mémorisation des TIC permet d'enregistrer les performances et de tracer en permanence les actions des collaborateurs* »[5].

[4] Aurélie Leclercq-Vandelnnoitte, Travail à distance et e-management, Organisation et contrôle en entreprise, Dunod, Paris, 2013

[5] Ibid

1.4. Les données personnelles

Périmètre

On désigne usuellement par "données à caractère personnel" les informations qui permettent d'identifier directement ou indirectement une personne physique. Ce sont principalement les nom, prénom, adresses physiques et électroniques, numéro(s) de téléphone, lieu et date de naissance, numéro de sécurité sociale, numéro(s) de carte de paiement, plaque d'immatriculation d'un véhicule, photos, empreintes digitales ou biométriques, données génétiques et médicales, etc.

À noter que la loi française interdit dans les fichiers soumis à l'autorisation de la CNIL, le stockage de certaines données de type origine raciale ou ethnique, les opinions politiques, philosophiques et religieuses.

Cadre juridique

Le cadre juridique en France et en Europe est déjà fourni et continue d'évoluer (cf. Annexe : cadre législatif relatif à la protection des données personnelles, page 25) :

- Loi Informatique et Liberté de 1978
- Obligations de la CNIL
- Directives européennes sur « Vie privée et communications électroniques » 95/46/CE & Convention n° 108

Il existe par ailleurs des réglementations propres à certaines professions : par exemple le secret médical, le secret bancaire, …

Un enjeu éthique majeur : respecter la vie privée dans le monde numérique

La protection de la vie privée se décline sous trois aspects :

- **Le droit au secret** : ne pas voir ses informations personnelles divulguées à son insu,
- **Le droit à l'anonymat** : rester protégé d'une attention ou observation par des tiers, non désirée,
- **Le droit à la solitude** : pouvoir choisir sa proximité physique par rapport aux autres.

Dans le monde numérique, le respect de ces droits est fragilisé.

Appliquée aux données personnelles se trouvant dans le monde numérique, la protection de la vie privée supposerait :

- de savoir et pouvoir contrôler quelles données sont stockées par quel(s) tiers, en vue de quel(s) traitement(s) – de l'affichage à des fins d'actions commerciales,
- d'être informé de la collecte de ces informations, et de pouvoir l'autoriser ou la refuser,
- d'être en mesure d'en obtenir à la demande le retrait et l'effacement.

Par les exemples ci-dessous, on voit comment certaines pratiques peuvent potentiellement entrer en conflit avec ces droits à la vie privée numérique, sans le consensus du client internaute.

	Droit au secret numérique	Droit à l'anonymat numérique	Droit à la solitude numérique
Divulgation de fichiers de prospects à des tiers (de la « coche » publicitaire, à la vente, voire au vol de fichiers)			
Acquisition sur les réseaux sociaux d'informations personnelles pour traitements de type profilage comportemental			
Imposition de publicités dites « personnalisées »			
Impossibilité à faire retirer / effacer les données non explicitement autorisées, impossibilité du droit à l'oubli			

Légende :

	Droits mis en danger
	Droits violés

En France et en Europe, les législations en vigueur sont protectrices de l'utilisateur/usager en matière de données personnelles : obligations CNIL (en France), autorisation demandée par les sites pour stocker des cookies, etc.

Au-delà du devoir moral vis-à-vis des salariés et des tiers, l'entreprise doit donc **s'assurer du bon respect de ses obligations à travers des dispositifs et processus mis en place, testés, et tenus à jour. C'est une obligation de conformité tout autant qu'un enjeu d'éthique**.

Il faut noter néanmoins que certaines entreprises internationales, dont de notables « géants du web », sont parfois peu, si ce n'est non soumises à des obligations réglementaires comme en France et en Europe.

1.5. Le Droit à l'oubli

Enjeux et interrogations

Le droit à l'oubli numérique soulève plusieurs problèmes :

- Le droit à l'oubli numérique ne signifie pas l'effacement définitif des données souhaitées ;
- Comment trouver le bon équilibre entre le droit à l'oubli et le droit à l'information?
- Le droit à l'oubli numérique dans ce cyber-village qu'est le monde numérique, n'est-il pas une gageure ? En théorie, beaucoup de solutions sont envisagées pour garantir le droit à l'oubli ; en pratique, nous observons une difficulté à régler et réglementer la problématique du droit à l'oubli numérique au sein d'un cyberespace où les lois sont multiples car spécifiques à chaque état.
- Octroyer systématiquement une durée maximale de détention de données personnelles, c'est indirectement accorder une forme d'oubli à l'individu concerné. Mais une question, qui reste ouverte, est de savoir comment gérer avec efficacité et efficience les durées de conservation des données ?

Malgré toutes ces incertitudes, une décision sur le « droit à l'oubli » a été adoptée par la Cour de justice de l'Union européenne (CJUE), rendue le 13 mai 2014. Pour la première fois, la Cour se prononce en faveur du droit à l'oubli numérique en demandant à Google d'adopter les mesures nécessaires pour retirer de son index des données à caractère personnel concernant un internaute et d'empêcher l'accès à celles-ci dans l'avenir.

Quelques jours après avoir mis en ligne un formulaire de demande d'effacement de lien, Google a reçu plus de 40 000 demandes des internautes.

Approche retenue dans l'entreprise — Témoignage du Groupe La Poste

La sensibilisation du plus grand nombre est une démarche nécessaire, avec deux cibles principales, qui sont de grands gestionnaires de données personnelles **: les Directions des Ressources Humaines et les Directions Marketing et Commercial (données client)**.

Les moyens de sensibilisation mis en place par Le *Groupe La Poste* se font au travers :

- d'ateliers thématiques,
- de formations internes,
- d'une boîte à outils sur le site web dédié à la protection des données personnelles.

L'entreprise opte pour un parti pris pédagogique. Elle a mis en place un certain nombre de documents et/ou de plateformes ludiques, faciles d'accès et compréhensible par tous :

QUIZZ

AFFICHE

SITE DEDIÉ À LA PROTECTION DES DONNÉES PERSONNELLES

Quelques expériences en cours :

- Depuis 2012, le travail avec les MOA (maîtrise d'ouvrage) sur l'expression des besoins devrait permettre **d'intégrer dès la conception des outils la gestion automatique des durées de conservation des données dans les nouvelles applications**.
- Une réflexion en cours au *Groupe La Poste* vise à définir « comment assurer pour nos clients un exercice plus facile de leurs droits, dont le droit à la suppression des données » : l'entreprise est pour le moment dans la phase d'analyse de l'existant. L'objectif est de **redonner aux clients le contrôle de leurs données**, tel que le voudrait le modèle du VRM (*Vendor Relationship Management*).

1.6. *Big Data* et données personnelles : quel équilibre entre enjeux *business* et enjeux éthiques ?

On évoque souvent la *data* comme étant désormais un actif stratégique de l'entreprise, voire l'or noir de l'économie numérique. Les enjeux commerciaux et publicitaires sont en effet considérables et permettent notamment plus de personnalisation à partir du traitement des données personnelles. Cependant certaines limites éthiques se dessinent face au déploiement de ces opportunités économiques et technologiques. Il convient d'avoir une **compréhension plus précise de ces enjeux éthiques afin de construire un modèle économique reposant sur la confiance des clients finaux**.

Interopérabilité des données et anonymat

L'enjeu avec les données personnelles aujourd'hui concerne non plus seulement leur gestion mais aussi et surtout **leur interopérabilité et leur hybridité**. C'est ce que déclare la CNIL dans son Cahier IP (Innovation et Prospective) *Vie privée à l'horizon 2020* : « *Si avec la naissance de la CNIL, les enjeux étaient le recueil de données pour de mauvais usages, aujourd'hui c'est l'interopérabilité qui est la nouvelle question centrale* »[6].

Arvind Narayanan, informaticien de l'Université de Princeton, suggère qu'avec **le *Big Data* et l'amélioration des outils d'analyse des données,** « ***l'anonymat est devenu algorithmi-***

[6] CNIL, *Vie privée à l'horizon 2020*, Cahiers IP, n°01, p.36.

quement impossible »[7]**.** C'est pourquoi aujourd'hui certaines instances de régulation, comme certaines CNIL européennes, se demandent si toutes les traces numériques que nous générons, comme les fichiers *cookies* par exemple, peuvent être considérées comme des données personnelles. L'adresse IP a déjà été reconnue par la Commission européenne comme étant une donnée à caractère personnel (car elle renvoie indirectement à une personne). Nous pouvons donc soutenir que **l'amélioration et la croissance des possibilités d'analyse des données repoussent sans cesse les limites de nos conceptions juridiques et éthiques de la vie et de l'espace privé.**

Exploitation commerciale des données personnelles

Recueillir des données sur nos habitudes de consommation est un procédé classique du marketing et ne constitue pas en soi une atteinte au respect de la vie privée. Mais la possibilité de traiter également tout l'écosystème des données et d'effectuer des croisements avec d'autres informations constitue un autre problème. Il semble aujourd'hui que la définition de la notion de « donnée personnelle » soit de plus en plus vaste et complexe à délimiter puisque leur hybridation permet la **déduction d'informations personnelles à partir d'algorithmes**. Le fait que ces informations ne soient pas **générées volontairement par un individu pose le problème de la maîtrise et du contrôle de ses données et de son identité numérique.** Il est en effet possible aujourd'hui de déduire à partir de données publiques (« *like* » sur Facebook, commentaires sur les réseaux et médias sociaux, …) des informations personnelles voire sensibles (conviction politique, religieuse, état de santé, …). Cela signifie donc que nous ne sommes plus maîtres du devenir de nos données sur internet : ceci remet en cause non seulement la notion de vie privée, mais aussi celle d'intimité puisque, même si à un premier niveau, nous pouvons régler nos paramètres de confidentialité, nous ne pouvons pas maîtriser par la suite les traitements externes qui hybrident les données et permettent de recueillir des informations personnelles. **La gestion des traces numériques et leur utilisation marketing engagent désormais de nouvelles responsabilités pour l'entreprise.**

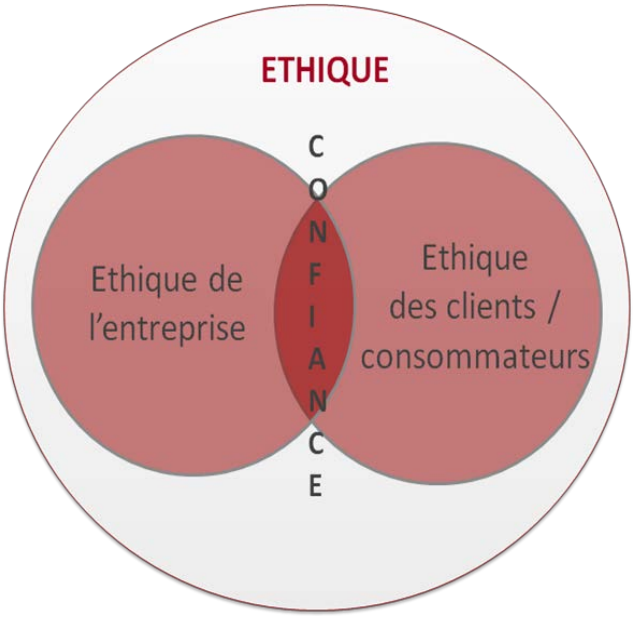
« A l'ère du Big Data, une grande partie de la valeur des données nait d'utilisations secondaires qui peuvent avoir été inimaginables lorsque les données ont été recueillies, ce qui signifie que le mécanisme de "notification et de consentement" pour assurer la confidentialité n'est plus adapté »[8].

---

[7] Cité par Hubert Guillaud (InternetActu.net), « Big Data, une nouvelle étape de l'informatisation du monde », 14.05.13

[8] Viktor Mayer-Schönberger et Kenneth Cukier, Big Data : une révolution qui va transformer notre façon de vivre, de travailler et penser, Houghton Mifflin, 2013

La confiance, une valeur essentielle à la pérennité du succès de l'entreprise numérique



La baisse de confiance des clients et des consommateurs envers les entreprises sur leur politique de traitement des données personnelles devient alarmante. Une récente étude d'Orange, *Futur of Digital Trust*[9], publiée en février 2014, nous enseigne qu'une grande majorité des consommateurs (78%) n'accordent que peu ou pas de confiance aux entreprises quant à la protection de leurs données personnelles.

Il devient urgent d'édifier un socle de valeurs communes entre l'éthique de l'entreprise et l'éthique des clients et consommateurs et ce autour d'une réelle transparence.

C'est parce que nous évoluons dans un univers où l'immédiateté et la connectivité font norme qu'il convient de réaffirmer certaines valeurs éthiques nécessaires au maintien de relations durables, à la confiance, au respect de la vie privée des collaborateurs et des clients. **Ce n'est qu'à travers ce juste milieu que nous pourrons construire une éthique commune entre l'entreprise et son écosystème et préserver la confiance.** Se donner soi-même des règles du jeu à respecter est aujourd'hui une nécessité qui dépasse de loin le simple respect de la règle de loi. Le nouveau défi pour l'entreprise numérique est de **trouver un terrain propice à la co-construction de valeurs éthiques.** L'équilibre entre les enjeux *business* et éthiques du traitement et de l'exploitation des données personnelles repose donc sur la confiance, valeur essentielle à la pérennité d'un modèle économique.

[9] Détails de l'étude : http://www.orange.com/fr/presse/communiques/communiques-2014/une-nouvelle-etude-souligne-la-mefiance-croissante-des-consommateurs-europeens-concernant-l-utilisation-de-leurs-donnees-personnelles

2. Élaboration d'un guide de recommandations « Éthique et Numérique »

2.1. Objectifs et Méthode

Les objectifs du groupe de travail « Éthique et Numérique » étaient de dresser un état des lieux de la réflexion éthique en rapport avec le contexte numérique des entreprises.

Suite à l'élaboration d'une réflexion commune, le groupe de travail a souhaité dresser un guide de recommandations à l'intention des entreprises. Le but n'est pas de fournir de réponses péremptoires sur les enjeux éthiques soulevés par le numérique, car nous considérons que l'éthique n'est pas qu'un produit (qui serait le code ou la charte), elle est essentiellement un processus, une capacité à réfléchir sur les valeurs, à s'interroger sur ce qui fait sens pour l'homme dans un contexte particulier.

De même, **l'appropriation des valeurs ou principes éthiques par l'ensemble des collaborateurs ne peut qu'être le fruit d'une réflexion commune, menée au sein de l'entreprise.** Cette démarche réflexive, nécessaire à l'élaboration ou à l'adaptation de ces recommandations, est propre à chaque entreprise, et à chaque secteur d'activité. C'est pourquoi, même si ce guide a une vocation pratique, il ne doit pas faire oublier l'essence même de l'éthique qui consiste à réfléchir et à faire réfléchir.

2.2. Contexte de la démarche

Une enquête CIGREF a été lancée en 2012 au sein de ses entreprises membres dans le but d'identifier des bonnes pratiques relatives au "droit des collaborateurs à la déconnexion" (ordinateurs, *smartphones*, messagerie, ...) et de savoir si, le cas échéant, elles auraient fait l'objet d'une charte.

Sur 12 entreprises répondantes, une minorité a défini des règles en matière d'usages des outils numériques. Les entreprises qui n'ont encore rien mis en place se déclarent concernées, dans leur grande majorité (83% des répondants), par le sujet de l'usage des outils numériques et du droit à la déconnexion : elles sont vivement intéressées par des exemples de chartes et de bonnes pratiques, car elles envisagent de (re)travailler sur ce sujet.

Les entreprises ayant défini des règles, voire mis en place une charte relative à l'usage des outils numériques (17% des répondants), se sont fixé comme objectif de définir quelques règles d'éthique, partagées par tous :

- La direction s'engage, vis-à-vis des collaborateurs, sur une série de points relatifs à l'emploi des outils numériques et aux bonnes pratiques associées.

- Les règles définies doivent être cohérentes avec les valeurs de l'entreprise et préciser les conduites managériales à tenir, telles que, dans un des exemples à notre disposition, le respect réciproque, la valorisation de la créativité et le discernement.
- L'usage des outils numériques peut être encadré par une charte qui couvre le respect de la vie privée des collaborateurs, le télétravail, les courriers électroniques, les réseaux sociaux et la communication associée, le *Bring Your Own Device*, et la responsabilité des utilisateurs vis-à-vis des informations qu'ils communiquent et publient.

Ces premières actions menées au sein des entreprises méritent d'être renforcées par un cadre plus précis et pratique. Néanmoins la définition de ce cadre n'est pas évidente et nécessite de comprendre les obstacles que rencontrent l'entreprise dans sa conception de l'éthique appliquée.

2.3. Comment faire une éthique appliquée au numérique ?

La prépondérance des technologies numériques en entreprise et leur usage dans la société fait résonner de nombreuses problématiques éthiques et suppose l'élaboration de nouveaux documents, chartes ou codes, spécifiques à l'usage du numérique. Une majorité d'entreprises a dû bâtir de nouvelles chartes éthiques en amont de la législation, dans le but d'affirmer des valeurs communes et propres au commerce sur internet, ou à l'utilisation des TIC au sein de l'entreprise.

L'éternel problème de l'éthique appliquée

Ceci ne va pas sans poser de nouveau la question de l'application de l'éthique en entreprise. Comment en effet rendre opérationnel des valeurs ou des principes ? Comme le remarque Philippe Goujon, professeur de philosophie à l'Université de Namur et directeur du LEGIT, « *l'identification des problèmes n'implique pas leur résolution* »[10]. Souvent la définition ou la communication des principes éthiques constitue la finalité ultime de la démarche éthique de l'entreprise.

Elle se heurte alors à plusieurs difficultés. D'une part, on occulte souvent le fait que la définition de principes constitue en elle-même un problème : qui est légitime pour définir ces principes ? Et comment faire converger la pluralité et la divergence des conceptions éthiques au sein d'une entreprise, qui plus est, d'une entreprise multinationale ?

D'autre part, la définition des principes n'implique pas nécessairement leur opérationnalité. C'est justement à ce niveau que se situe le problème pour les entreprises soucieuses de

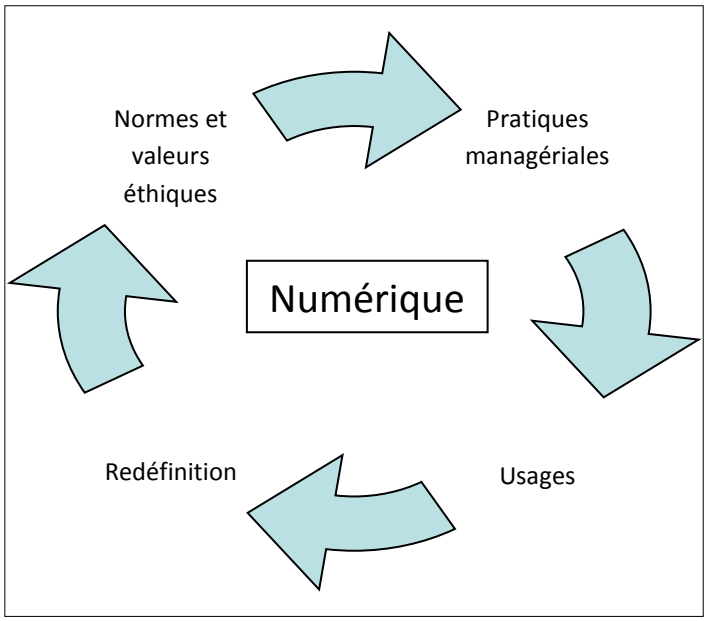
[10] Intervention au colloque CIGREF « Éthique et Numérique : quels enjeux pour l'entreprise ? », le 28 mars 2014

« faire appliquer » l'éthique. **La non-effectivité des principes éthiques vient souvent de leur abstraction et de leur non-appropriation par les collaborateurs.** D'où l'importance, nous semble-t-il, **d'impliquer un maximum de personnes dans la définition de ces principes éthiques**, d'encourager la réunion des acteurs de l'entreprise pour aborder ces sujets dans un esprit de réflexion, de co-création, en impliquant les métiers et les fonctions supports.

Prendre en compte la spécificité du numérique

L'éthique appliquée se définit toujours en fonction du contexte dans lequel elle évolue. L'éthique appliquée au numérique naît de questionnements issus des changements et évolutions sociétaux et/ou technologiques de l'entreprise. **Cette éthique exige de mener une démarche de réévaluation des valeurs et des normes à partir des changements observables dans la vie de l'entreprise.**

On peut trouver deux modèles existants concernant les modes d'application de l'éthique dans la littérature managériale : *top-down* et *bottom-up*. Soit l'on considère que l'éthique normative doit être simplement « appliquée » à des comportements ou à des situations, soit on considère au contraire qu'il faut définir l'éthique normative à partir de certaines pratiques. Mais cette binarité est réductrice selon Malik Bozzo Rey, professeur de philosophie et responsable du Centre de recherche Éthique Économique Entreprise à l'Université de Lille[11]. A l'opposé de ces deux modèles verticaux, Malik Bozzo Rey propose un **modèle circulaire** : l'éthique normative va influencer les pratiques, et dans un même mouvement les pratiques vont permettre l'interrogation permanente de ces normes. **Ce modèle circulaire devrait faciliter l'interaction entre théories éthiques, pratiques managériales et usages du numérique**. De plus, les technologies numériques peuvent soutenir cette mise en relation, car elles exacerbent la transmission d'informations et de collaboration au sein de l'entreprise, et iraient même jusqu'à la construction d'un « cerveau global » selon Malik Bozzo Rey.



[11] Intervenant lors du colloque CIGREF « Éthique et Numérique : quels enjeux pour l'entreprise ? », le 28 mars 2014

3. Guide méthodologique et pratique

Nous pouvons alors proposer **quatre étapes structurantes pour élaborer une réflexion éthique dans l'entreprise.**

3.1. Étapes

Interrogation & Compréhension

Pour comprendre les risques éthiques spécifiques au contexte numérique, il faut avant tout :

- **S'interroger sur la transformation du contexte sociotechnique de l'entreprise** et son influence sur les comportements individuels, sociaux, professionnels etc... **Le rôle du manager est essentiel dans l'accomplissement de cette première étape.**
- **Faire des études, au plus près du terrain, en interne,** sur les conséquences sociales, éthiques et humaines de la mise en place de nouveaux outils numériques et de leur usage en entreprise : quelles modifications dans les rythmes de travail ? Quelle influence sur le brouillage des frontières vie privée/ vie professionnelle ? Observe-t-on de nouvelles fractures d'usage et/ou générationnelles ?
- **Effectuer des enquêtes ou s'informer auprès des clients et plus généralement des parties prenantes,** afin **d'évaluer le niveau d'acceptabilité sociale** concernant par exemple l'exploitation commerciale des données personnelles, les innovations technologiques et les nouveaux usages qui les accompagnent, etc.

Identification

- Se demander si chaque individu est capable **d'identifier les enjeux éthiques propres à sa fonction ou à son corps de métier**.
- Consulter les fonctions supports et les Directions Métiers afin d'identifier leurs enjeux respectifs.
- Mettre en place **des comités transversaux, *cross*-métiers** afin de faciliter l'identification et la mise en commun des (futures) responsabilités à définir.

Construction & Implication

- **Se demander comment les valeurs se construisent et s'approprient** : un document, charte ou code, est-il suffisant pour sensibiliser aux enjeux éthiques ?
- **Organiser des groupes de travail / de réflexion** sur la définition des valeurs éthiques et y faire participer un maximum de collaborateurs, de tous niveaux, afin de faciliter l'appropriation des valeurs définies.

- **Définir une instance interdisciplinaire** composée de juristes, CIL[12], RH, chercheurs, …, chargée de l'éthique dans chaque secteur d'activité de l'entreprise — s'il n'existe pas déjà de comité éthique ou de service déontologie.
- **Renforcer la relation du CIL avec l'ensemble des collaborateurs** : si son rôle est essentiellement de veiller à la conformité des activités de l'entreprise en matière de données personnelles et de conseiller les responsables des traitements de données, il pourrait aussi être un **relai d'informations** privilégié **auprès des collaborateurs concernés à tous les niveaux de la hiérarchie**, et **favoriser ainsi plus largement la diffusion de la culture "informatique et libertés"** (recommandations CNIL, actualité juridique, comportements éthiques, réflexions dans les *Think Tank*, etc.) à travers la mise en place d'espaces dédiés, ou à travers les comités d'éthique des entreprises.

Influence & Diffusion

- **Identifier les influences de chaque secteur de l'entreprise en termes d'éthique** : DG, Métiers, Gouvernance. Faut-il nécessairement formaliser l'éthique pour la diffuser ou compter sur l'influence d'un manager ou d'une équipe ?
- **Les comités éthiques sont des vecteurs d'influence et de diffusion** : ils peuvent aider les acteurs à définir leurs rôles et leurs responsabilités. Pour cela le comité éthique peut :
  - Faire le lien avec la politique SSI[13] et les chartes d'usage du numérique déjà en place ;
  - Intégrer ces nouveaux enjeux à la gouvernance du numérique ;
  - Impliquer les métiers, et les RH en particulier, dans l'accompagnement au changement car le numérique crée de nouveaux usages et de nouveaux comportements, et implique de ce fait de faire évoluer les pratiques, particulièrement les pratiques managériales ;
  - Compléter les chartes/codes de déontologie des entreprises pour prendre en compte les nouveaux enjeux du numérique (réseaux sociaux, mobilité, gestion des données, etc.), et les diffuser largement ;
  - Faciliter la diffusion en rendant les chartes/codes ou pratiques accessibles (traduction dans différentes langues), lisibles, pédagogiques voire ludiques.

[12] Correspondant Informatique et Libertés. Selon une nouvelle réglementation européenne (2013), le CIL deviendra d'ici 2016, un DPO (*Data Protection Officer*) : ses fonctions seront accrues notamment au niveau juridique et il aura un rôle majeur dans la restitution des données personnelles aux utilisateurs. Nommer un CIL / DPO dans son entreprise devient un véritable signe d'engagement éthique, favorisant ainsi la relation de confiance avec les clients

[13] Sécurité du Système d'Information

3.2. Thèmes

L'élaboration des recommandations s'appuie sur quatre grands axes, que l'on trouve de manière récurrente dans les chartes éthiques des entreprises : **protection des salariés, protection des clients, protection du patrimoine, et rôle citoyen de l'entreprise dans son environnement**. La description de ces thématiques à travers le prisme du numérique donne un cadre à l'élaboration de nos recommandations.

Protection des salariés

- **Respect de la vie privée, droit à la déconnexion**

Le respect de la vie privée peut être remis en cause par la facilité qu'occasionnent les outils numériques à rendre de plus en plus perméables les espaces entre vie professionnelle et vie privée. Il faut donc avoir conscience que le respect de la sphère privée des collaborateurs et de tous les utilisateurs de l'entreprise doit faire l'objet d'une attention particulière car les outils numériques permettent une connexion et une sollicitation à tout instant et la mobilité des outils accentue ce risque. C'est donc un enjeu essentiel au maintien du bien-être des personnes et des bonnes relations au travail.

- **Égalité d'accès et d'usage : la fracture numérique**

Aujourd'hui, la fracture numérique est moins une question d'accès, bien qu'elle soit toujours présente, qu'une question d'usage et d'appropriation qui peut générer des inégalités : la façon dont chacun va chercher et traiter une information en fonction d'un besoin précis, ou gérer ses paramètres de confidentialité va dépendre de sa capacité d'usage et de sa connaissance de l'outil.

Cette fracture d'usage pose problème aujourd'hui notamment au travers de la mise en place d'outils de calcul d'influence numérique, lesquels permettent de repérer les potentialités des individus par rapport à leur activité sur les réseaux sociaux de l'entreprise et/ou publics. Or avec les fractures d'usage il faut prendre en compte le fait que nous ne sommes pas tous égaux face à ces nouvelles techniques de notation ou d'appréciation du travail d'un employé.

Protection des clients

- **Protection des données personnelles, droit à l'oubli**

Le traitement des données personnelles est une problématique majeure aujourd'hui et dont l'importance ne cesse de croître au regard des innovations technologiques. Les utilisateurs (clients, consommateurs) sont de plus en plus soucieux de savoir quelles informations sont détenues sur eux et quel usage en est fait par l'exploitant. **Cette problématique devient un enjeu de réputation pour les entreprises et fournisseurs**. Si l'usage des données recueillies n'est pas conforme à la politique revendiquée par l'entreprise, ou si la finalité du traitement

des données est détournée à de fins commerciales, sans accord préalable et explicite du client, la méfiance des utilisateurs risque en effet de s'accroître considérablement, et la réputation des entreprises et/ou fournisseurs peut en pâtir.

La réclamation d'un droit à l'oubli pose de nouvelles conditions aux entreprises et notamment aux *pure players*. En effet, aujourd'hui, plus une entreprise accumule de données plus elle a de chances de créer de la valeur. L'entreprise doit aujourd'hui trouver un équilibre entre l'enjeu *business* et l'enjeu éthique que recouvre l'exploitation des données personnelles. La performance des outils numériques actuels repose sur la mémoire, la capacité à se souvenir et à créer des recommandations personnalisées. En revanche, l'une des principales caractéristiques de l'homme c'est l'oubli. Nietzsche fut d'ailleurs l'un des premiers à considérer que l'oubli, « l'oubli positif », est une faculté nécessaire au bien-être de l'homme. L'oubli est donc quelque chose de non naturel pour la technologie, d'où l'importance d'en faire un « droit » humain.

- **Transparence, cohérence et pédagogie**

Vis-à-vis de ses clients, l'entreprise peut expliciter le plus clairement possible sa politique de traitement des données personnelles, et la rendre accessible en mettant en ligne les règles qu'elle s'engage à respecter sur l'usage des données clients. Elle fait ainsi preuve non seulement de transparence, mais aussi de cohérence avec ses valeurs qui sont le plus souvent présentes dans les chartes éthiques (honnêteté, intégrité, respect…), et de pédagogie en faisant l'effort de rendre ses règles lisibles et compréhensibles (c'est-à-dire qu'elles ne soient pas écrites avec une police de trop petite taille, ou en employant un vocabulaire trop technique) par un plus grand nombre.

Protection du patrimoine

Le numérique amplifie certains problèmes déjà existants : la protection des données et des informations en est un parfait exemple. Il devient primordial pour l'entreprise de renforcer la protection de ses données patrimoniales en sensibilisant les employés aux risques de sécurité liés à l'utilisation de ces données. Il s'agit également d'insister sur le devoir des acteurs à l'égard de l'entreprise, et le rôle qu'ils ont dans la protection du « secret de fabrique ». Mais la protection du patrimoine ne traite pas seulement des données. C'est l'ensemble des actifs de l'entreprise qui sont concernés, y compris les biens vendus aux clients. Les réseaux numériques peuvent permettre en effet à des personnes mal intentionnées, de prendre le contrôle à distance d'équipements insuffisamment protégés : ordinateurs, machines, installations et toutes sortes d'objets connectés, par exemple des véhicules de tous types.

Le rôle citoyen de l'entreprise dans son environnement

L'entreprise doit se préoccuper de l'impact négatif que pourrait avoir son activité et ses produits finis sur son environnement. L'acceptabilité sociale est aujourd'hui une question de réputation. La transparence de l'entreprise concernant ces sujets est cruciale.

Le numérique a en effet un caractère pharmacologique et peut être à la fois potion et poison. C'est le cas pour toute innovation technologique majeure :

- Les lunettes Google associés au « *Big Data* » ouvrent de nouvelles perspectives quant à la personnalisation des recommandations et permet une meilleure stimulation du client grâce à la réalité augmentée, mais soulève également de nombreuses interrogations autour de l'anonymat et du libre arbitre. L'exemple de Google nous montre que nos capacités d'analyse, de réflexion et de choix peuvent être prises en charge par des technologies adaptées. Si les algorithmes permettent de manipuler ou détourner notre attention au travers de recommandations personnalisées, voire de prédire certains comportements, qu'advient-il de notre libre arbitre ?
- Les objets connectés prennent une importance croissante dans le développement de nos sociétés et des entreprises. Ils peuvent avoir des fonctions utilitaires et salvatrices dans certains domaines : par exemple, pour les forêts exposées à des risques d'incendie, il existe désormais des relais de capteurs qui permettent de détecter et de transmettre instantanément le déclenchement d'un feu. Mais le déploiement des objets connectés à l'ensemble de la société soulèvent de nombreuses questions relatives au « traçage » de l'individu : la capacité de ces objets à interagir avec leur environnement suppose que les données collectées seront de plus en plus personnelles. Les données de mobilité recueillies révèlent même davantage d'informations personnelles sur un individu que son propre ADN[14].
- Les imprimantes 3D vont poser le problème de la copie illicite de pièces de rechange.
- Les voitures connectées vont apporter de nouveaux services aux passagers, mais peuvent ouvrir aussi la possibilité à des *hackers* de prendre les commandes du véhicule.

Une entreprise qui souhaite distribuer ces nouvelles technologies numériques a le devoir d'en évaluer les risques potentiels, d'en informer les autorités et les clients, et de proposer des parades.

[14] Etude du MIT *Unique in Crowd : The privacy bounds of human mobility*

3.3. Guide de recommandations

Les recommandations qui suivent ont été élaborées selon deux catégories : les droits et les devoirs. Elles s'adressent aux managers et aux utilisateurs, mais aussi à l'entreprise dans sa conception « étendue », c'est-à-dire aux fournisseurs et partenaires commerciaux.

Ce guide n'a pas prétention à être exhaustif. Il donne un cadre général et présente certaines pratiques que l'on peut déjà trouver dans certaines chartes d'entreprise. Pour aller plus en profondeur dans la réalité concrète de ces recommandations, nous souhaitons signaler l'existence de documents pertinents et fournissant un cadre précis et spécifique à chaque sujet :

- *Le Guide AXA du Bon Sens Numérique - Les 20 conseils indispensables pour faire preuve de Bon Sens Numérique sur les médias et les réseaux sociaux* : http://www.axaprevention.fr/Documents/fichiers_pdf/AXA_GUIDE_BSN.pdf
- *Charte Éthique et Big Data*, à l'initiative de APROGED, ATALA, AFCP et CAP DIGITAL, 2013 : http://www.blogbigdata.com/wp-content/uploads/2013/05/Charte_Ethique_BigData.pdf
- *La bonne utilisation de l'e-mail dans l'entreprise*, MEDEF, 2008 : http://www.medef.com/medef-corporate/publications/fiche-detaillee/categorie/economie-1/back/110/article/la-bonne-utilisation-de-le-mail-en-entreprise.html
- *Usage des TIC et RSE : nouvelles pratiques sociales dans les grandes entreprises*, Rapport CIGREF - ORSE, 2009 : http://www.cigref.fr/usage-des-tic-et-rse-nouvelles-pratiques-sociales-dans-les-grandes-entreprises-en-partenariat-avec-lorse-2
- Recommandations et obligations de la CNIL: http://www.cnil.fr/documentation/deliberations/recommandations/

Protection des salariés

MANAGERS	UTILISATEURS FINAUX (collaborateurs, stagiaires, apprentis, intérimaires, prestataires, …)
DEVOIRS	
• Ne pas appuyer les décisions de recrutement sur les informations d'ordre privé qui pourraient être disponibles sur le web (Facebook, Twitter, etc.) • Ne pas exploiter ou divulguer les données personnelles que les salariés auraient pu enregistrer sur leur poste de travail • Mettre en place les dispositifs organisationnels (service déontologie…), et les outils permettant de recueillir et d'instruire les alertes professionnelles • Mettre en place les dispositifs facilitant l'accès des collaborateurs à leurs données • Proposer des espaces de travail favorisant le bien-être au travail • Ne pas déranger les collaborateurs par des mails, sms, messages instantanés, appels sur mobile, etc., en dehors de leurs horaires de travail ou d'astreinte, sauf en cas d'urgence avérée • Ne pas mettre en place de systèmes de notation / surveillance / contrôle sur la base d'un traitement de données personnelles sans en avertir l'employé • Protéger les données sur les salariés • Informer les salariés sur les règles de bon usage de l'Internet, et encadrer strictement les raisons légales qui pourraient conduire à un examen de leur historique d'accès à Internet et de leurs échanges de données avec le Web (download, upload)	• Respecter les règles de confidentialité, et les chartes d'usage • Se former aux nouveaux outils de travail et aux nouvelles pratiques, liés à l'évolution de leur métier • Respecter le guide d'usage des ressources numériques, définissant les règles de bonne conduite à appliquer et avoir connaissance des sanctions éventuelles en cas de non-respect de ces règles (à détailler dans une charte)

Protection des salariés	
MANAGERS	**UTILISATEURS FINAUX** (collaborateurs, stagiaires, apprentis, intérimaires, prestataires, …)
DEVOIRS	
• Mettre en place des programmes de formation génériques sur le numérique, pour tous les salariés • Adapter les postes de travail pour les salariés souffrant d'un handicap physique ou cognitif et les former • Développer l'accessibilité numérique[15] des documents et sites web	
DROITS	
• Disposer des moyens pour faire respecter les règles en vigueur (charte éthique, règles d'usage des outils numériques, …) : formations, moyens de contrôle • Etre formé à la prise en compte et à la gestion de ces nouveaux risques. • Etre assisté dans la mise en œuvre des bonnes pratiques et soutenu dans la gestion des situations complexes/difficiles.	• Demander à être formé au cadre réglementaire spécifique au numérique. • Disposer d'outils adaptés en cas de handicap. • Signaler les phénomènes de Cognitive Overflow Syndrome (surcharge informationnelle et cognitive) et de burn-out (surmenage). • Disposer d'un environnement de travail propice au développement des relations interpersonnelles (espaces détente, groupes de parole, médiation…) pour anticiper les situations de stress que le numérique favorise en sur-sollicitant les personnes.

[15] L'accessibilité numérique est la mise à disposition de tous les individus, quels que soient leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales, des ressources numériques.(source Wikipedia)

Protection du patrimoine

MANAGERS	UTILISATEURS FINAUX (collaborateurs, stagiaires, apprentis, intérimaires, prestataires, …)
DEVOIRS	
• Prendre toutes les mesures nécessaires pour garantir la confidentialité et l'intégrité des données, ainsi que la disponibilité des systèmes d'information dans le cadre des contrats de service définis avec ses clients internes ou externes • Respecter la classification des données de l'entreprise en fonction de leur niveau de criticité • Attribuer aux collaborateurs habilités à utiliser des données sensibles, les moyens de protection nécessaires pour appliquer les règles (par exemple, des outils de chiffrement) • Nommer un responsable de la veille sur l'e-réputation de l'entreprise et lui fournir les outils et informations nécessaires à l'élaboration des réponses sur le web	• Utiliser les outils de protection mis à leur disposition • Connaître et respecter la politique de sécurité des SI en place • Alerter la hiérarchie sur les pertes d'informations
DROITS	
• Etre sensibilisé à la protection des données, en particulier dans les cas de mobilité et du • Etre formé au cadre réglementaire en vigueur et à son évolution.	

Rôle citoyen de l'entreprise dans son environnement	
MANAGERS	**UTILISATEURS FINAUX** (collaborateurs, stagiaires, apprentis, intérimaires, prestataires, …)
DEVOIRS	
• Évaluer les risques potentiels des innovations technologiques, en assumer la responsabilité en informant les autorités et les clients et en proposant des parades • Développer un système d'information frugal en appliquant les bonnes pratiques d'éco-conception des logiciels • Intégrer la dimension éco-conception dans les appels d'offres	• Avoir un usage frugal des postes de travail (PC, imprimantes, etc.) par exemple, en éteignant son poste en cas d'absence prolongée ou en n'imprimant que le juste nécessaire

Protection des clients

MANAGERS	UTILISATEURS FINAUX (collaborateurs, stagiaires, apprentis, intérimaires, prestataires, …)
DEVOIRS	
• S'interdire de diffuser de fausses informations sur les médias sociaux, sur les forums spécialisés, sur les sites web de l'entreprise ou ceux de ses concurrents • Garantir une protection totale des données confidentielles confiées par les clients. Chiffrer les données critiques (comme les coordonnées bancaires) • Informer les clients sur les données nominatives que l'on a l'intention de conserver et sur l'usage que l'on souhaite en faire. Obtenir leur accord formel • Effectuer les déclarations règlementaires à la CNIL (ou organisme équivalent) sur les données clients gérées dans les bases de l'entreprise, et sur l'usage que l'on en fait • S'assurer que les demandes faites par le client, de rectification et de suppression de ses données, sont bien transmises aux tiers	• S'interdire de diffuser de fausses informations sur les médias sociaux, sur les forums spécialisés, sur les sites web de l'entreprise ou ceux de ses concurrents • Ne s'autoriser à transmettre les données personnelles à des tiers qu'après accord explicite du client • Donner le choix au client d'accepter ou non un processus de traitement de données personnelles • Faciliter l'accès des clients à leur données, rendre accessibles et compréhensibles les chartes et règles concernant la protection des données personnelles. Favoriser une démarche pédagogique • Définir clairement la ou les finalité(s) des traitements des données à caractère personnel
DROITS	
• Mettre en ligne publiquement les règles et politiques de traitement des données personnelles, les rendre lisibles, compréhensibles par tous	

ANNEXE : Cadre législatif relatif à la protection des données personnelles

Ce tableau récapitulatif sur le cadre réglementaire actuel est tiré du guide co-réalisé par l'IFA et le CIGREF, *Le conseil d'administration et la transition numérique de l'entreprise*, paru en septembre 2013[16].

Textes législatifs relatifs à la protection des données personnelles (non exhaustif)

Protection des données personnelles				
Texte	**Faits visés**	**Sanctions**	**Objet ciblé**	**Personnes**
Art. 34 Loi Informatique, Fichiers et Libertés + Art. 226-17 Code pénal + Art. 30 du projet de Règlement en matière de DCP RISQUE PENAL	Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978.	**Peine d'emprisonnement** : 5 ans de prison **Amende** : 300.000 € (X 5 lorsque les faits sont commis par une personne morale)	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE Dirigeant de la personne morale** qui n'a pas mis en place les conditions de sécurité concernant les traitements de données à caractère personnel & Personne morale selon l'art. 323-6 du Code pénal
Art. 34 bis Loi Informatique, Fichiers et Libertés + Art. 226-17-1 Code pénal +Art. 31 et 32 du projet de Règlement en matière de DCP	Absence de notification d'une violation de données à caractère personnel à la CNIL ou l'intéressé.	**Peine d'emprisonnement**: 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**VICTIME Les dirigeants, personnes** dont les données à caractère personnel ont été accédées du fait de failles de sécurité découlant des manquements d'un fournisseur de services de communications électroniques

[16] Disponible ici : http://images.cigref.fr/Publication/2013-IFA-CIGREF-Conseil-d-Administration-et-Transition-Numerique-d-Entreprise.pdf

Protection des données personnelles				
Texte	**Faits visés**	**Sanctions**	**Objet ciblé**	**Personnes**
Art. 226-18 Code pénal + Art. 5 du projet de Règlement en matière de DCP	Collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** **Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**
Art. 226-18-1 Code pénal + Art. 19 du projet de Règlement en matière de DCP	Procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes.	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** **Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**
Art. 226-19 Code pénal + Art. 9 du projet de Règlement en matière de DCP	Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation ou identité sexuelle de celles-ci. Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.	**Peine d'emprisonnement :** 5 ans de prison **Amende** : 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** **Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**

Protection des données personnelles				
Texte	**Faits visés**	**Sanctions**	**Objet ciblé**	**Personnes**
Art. 226-20 Code Pénal +Art. 5 du projet de Règlement en matière de DCP	Conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi. Le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE Personne chargée de la collecte et du traitement** des données personnelles **Personne morale** selon l'art 226-24 du Code pénal
Art. 226-22 Code pénal +Art. 6 du projet de Règlement en matière de DCP	Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir.	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 € La divulgation est punie de **3 ans d'emprisonnement** et de **100 000 € d'amende** lorsqu'elle a été commise par imprudence ou négligence	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**

Protection des données personnelles				
Texte	**Faits visés**	**Sanctions**	**Objet ciblé**	**Personnes**
Art. 226-22-1 Code pénal +Art. 40 du projet de Règlement en matière de DCP	Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n°78-17 du 6 janvier 1978 précitée.	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** Personne chargée de la collecte et du traitement des données personnelles Personne morale

Textes législatifs relatifs à la protection des données personnelles par secteur d'activité (non exhaustif)

Protection des données personnelles par secteur d'activité				
Textes	**Faits visés**	**Périmètres d'application** (secteur, société etc.)	**Code applicable**	**Personnes responsables**
Hébergement de données de santé : loi Kouchner	Procédure d'agrément des hébergeurs qui gèrent des données de santé à caractère personnel. Conformément au décret, l'hébergeur se doit : - d'organiser le dépôt des données de santé dans un environnement garantissant leur pérennité et leur confidentialité ; - de mettre en place des mesures garantissant la sécurité des informations de santé (traçabilité, archivage, sécurité des SI et contrôle des droits d'accès). Le ministère délivre un agrément tous les 3 ans, avec implication de la CNIL dans la délivrance de l'agrément.	Hébergeurs de données de santé	Décret n°2006-6 du 4 janvier 2006	Direction Générale Direction des Systèmes d'Information
ARJEL	Agréments accordés aux opérateurs de jeux en ligne et dont les conditions d'obtention sont soumises à la sécurisation et la traçabilité des informations des joueurs réputés français. La loi prévoit que chaque agrément donne lieu à la mise en place d'un dispositif technique qui permet de garantir une traçabilité des opérations de jeu d'une part, et de générer et de transmettre des rapports sur l'activité de jeu d'autre part.	Opérateur de jeux en ligne (paris hippiques, paris sportifs, jeux de cercles)	Décret n° 2010-482 du 12 mai 2010 - Conditions de délivrance des agréments d'opérateur de jeux en ligne	Direction Générale
CNIL : loi I&L de 1978	Cette loi concerne toute forme d'organisation et couvre la traçabilité, l'archivage et la sécurité des accès à l'information + proposition de règlement européen sur la protection des données à caractère personnel. - Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques	Toutes formes d'organisation	Loi 78-17 1978-01-06 art. 34	Propriétaire des fichiers ou des traitements informatiques de données à caractère personnel

Protection des données personnelles par secteur d'activité				
Textes	**Faits visés**	**Périmètres d'application** (secteur, société etc.)	**Code applicable**	**Personnes responsables**
	(sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. - Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des «tiers autorisés» ayant qualité pour les recevoir de façon ponctuelle et motivée (ex.: la police, le fisc). - Les données personnelles ont une date de péremption. Le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier. - Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer: son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées. - Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL. - Un fichier doit avoir un objectif précis. Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif. Les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.			

CIGREF

21 avenue de Messine

75008 PARIS

Tel. : +33 1 56 59 70 00

Fax : +33 1 56 59 70 01

cigref@cigref.fr

www.cigref.fr