A N D S I

Association Nationale des Directeurs des Systèmes d'Information
www.andsi.fr

La responsabilité pénale du DSI, en particulier en regard du (futur) règlement Européen sur les données personnelles.

par

Me André MEILLASOUX
ATM Avocats, Président de l'AFDIT (Association Française de droit de l'Informatique et de la Télécommunication), accompagné de Me Alban BÉGUÉ, ATM Avocats.

Séance du 19 mars 2013

En bref…

Les DSI font face à une situation nouvelle, le décloisonnement, c'est-à-dire la chute les digues construites pour canaliser les besoins et donc contrôler les solutions IT, auquel se conjugue une « industrialisation » de grande ampleur qui concerne tous les aspects de la profession.
L'externalisation, en particulier des fonctions techniques, et la progression d'offres telles que Saas, Paas, IaaS… conduit vers un modèle orienté revente de services, au détriment du modèle actuel encore majoritairement basé sur la fourniture directe de services aux utilisateurs.
Face à des prestataires informatiques, le DSI doit veiller à une relation contractuelle parfaitement cadrée.
En interne le décloisonnement engendre des obligations et des risques auxquels il est exposé sur un plan professionnel mais également sur un plan civil voir pénal.
Le dirigeant d'entreprise aura tout intérêt à procéder à une délégation de pouvoir, au DSI d'être vigilant dans la forme de contractualisation que présentera cette délégation.
La protection des données à caractère personnel est devenue un sujet majeur. Sa collecte et son traitement font l'objet d'obligations par la CNIL qui seront relayées, et peut être amplifiées, par le futur règlement européen en 2014-2015.
Dès lors la rigueur, qualité reconnue d'un DSI, doit elle être particulièrement utilisée pour sécuriser sa fonction en interne mais également par rapport à ses relations extérieures.

Exposé de André Meillassoux

Introduction

André MEILLASSOUX présente ses différentes activités dont 60 % sont consacrées à la négociation de contrats informatiques entre des clients et des fournisseurs de prestations informatiques.
L'industrie informatique a pas mal souffert ces dernières années concernant les difficultés rencontrées dans la mise en œuvre d'ERP nécessitant une vigilance dans la négociation de ce type de contrats pour clarifier au mieux les différentes responsabilités notamment l'identification d'un réel *« maitre d'œuvre ».*
Le modèle économique des éditeurs que l'on a connu change avec notamment le concept de *cloud.*
On voit apparaître par exemple la notion de « *paiement à la consommation* ».
Ces évolutions nous interpellent sur le rôle et les responsabilités des DSI.

Eléments de contexte

Les DSI se trouvent au carrefour de nombreux flux d'informations échangés avec les nombreux acteurs de l'entreprise.
On voit ainsi s'accroitre au cours du temps des obligations et des risques pesant sur les DSI.
Les raisons sont multiples :

- intrusion des technologies dans toutes les couches de l'entreprise ;
- prise de conscience des risques induits par les techniques ;
- souci sociétal d'accroitre les responsabilités, en touchant les personnes physiques ;
- multiplication des initiatives législatives aggravant les responsabilités des dirigeants d'entreprise.

Les principales conséquences sont les suivantes :

- une législation dispersée induisant des risques mal identifiés à tous les niveaux ;
- obligation des dirigeants d'entreprise à transférer certaines responsabilités vers des directions fonctionnelles comme les DSI.

⇨ **Les DSI doivent doter leur entreprise d'un réseau d'échanges opérationnel et sécurisé et également communiquer sur les changements organisationnels et techniques induits par ces contraintes techniques et juridiques.**

- Quel type de responsabilité sur le plan civil et pénal encourt le DSI ?
- Comment ces différents risques pèsent sur le DSI ou sur l'entreprise ?
  - jusqu'ou peut aller leur systématisation ?
  - quelles sont les conséquences sociétales sur la gestion des données personnelles ?
- Comment intégrer le projet de réglementation européen ?
- …

Autant de questions à se poser et de réponses à apporter.

Me André MEILLASSOUX propose d'aborder les points suivants :

- les principes de la responsabilité juridique ;
- la délégation de pouvoirs ;
- la responsabilité du DSI ;
- les moyens de prévention.

Les principes de la responsabilité juridique

Il y a lieu de distinguer la responsabilité des personnes morales de celle des personnes physiques.
La personne morale représentée souvent par un organe (groupe de personnes physiques) est responsable même si l'organe a dépassé ses pouvoirs.
Sa responsabilité peut engager celle de personnes physiques qui composent l'organe.
Les sanctions peuvent être professionnelles, ou relevant du droit civil voire pénal.

La délégation de pouvoirs

En pratique le dirigeant d'entreprise (*le délégant*) est donc amené à déléguer certains pouvoirs à son DSI (*le délégataire)*.
Cette délégation (qui n'a rien à voir avec une délégation de signature) doit :

- répondre à certaines obligations tant au niveau du délégant qu'à celui du délégataire ;
- être écrite en précisant le périmètre et identifier les risques juridiques encourus.

Elle peut toutefois être privée d'effets en cas de faute personnelle du délégant.

⇨ *Une question est posée aux DSI présents: combien d'entre eux ont-ils connu, au cours de leur carrière, une délégation ayant fait l'objet d'un document écrit ? Réponse : plus de 15%*

La responsabilité du DSI

Le DSI peut voir sa responsabilité civile ou pénale engagée, voire les deux cumulativement. Il peut engager sa responsabilité professionnelle en interne, au regard de l'application du code du travail.

Quels peuvent être les différents risques encourus ?

Ils concernent principalement :

- toutes infractions pénales commises par les salariés à partir de leur accès aux ressources informatiques de l'entreprise et au réseau (diffamation, fraude, escroquerie, propos racistes, délits sexuels…) ;
- la contrefaçon / le piratage (logiciels, contenus, etc.) ;
- l'intrusion non autorisée d'un salarié de l'entreprise dans un autre système d'information à partir des moyens fournis par son employeur ;
- la cybersurveillance sur les lieux de travail (la loi informatique et libertés) ;
- l'atteinte à un secret de fabrique ;
- le non-respect des règlementations financières / défaut de conformité aux textes en vigueur (SOX, LSF, IAS…) ;
- l'archivage et la sauvegarde des fichiers…

Le traitement des données personnelles mérite, parmi ces risques, un focus particulier

Le périmètre de ses responsabilités (induit par délégation) est le suivant :

Domaines couverts	Délits possibles	La violation de ces obligations est passible de 5 années d'emprisonnement et 300.000 euros d'amende
La sécurité des données	Le non-respect de l'obligation de sécurité	
La confidentialité des données	• La collecte non autorisée de données personnelles ou la collecte de données sensibles hors les cas prévus • Le détournement de données personnelles • La divulgation d'informations à des personnes non-autorisées	
L'information des personnes concernées	Le refus ou l'entrave au bon exercice des droits des personnes	
La suppression des données lorsque leur conservation n'ont plus lieu d'être	La conservation des données au-delà de la durée déclarée	
L'information de la CNIL, avant la mise en œuvre du traitement, lorsque les données présentent des risques particuliers d'atteinte aux droits et aux libertés.		

Réforme de la directive « données personnelles » : Règlement Européen en 2014-2015

S'il y a une volonté indéniable d'harmoniser les protections et de renforcer la sécurité des données personnelles, il faut noter la pression exercée par les lobbys américains, présents au Parlement Européen, pour réduire la portée de ce qui constituera le futur règlement européen.

⇨ **Ce qui change en droit :**

- introduction de nouveaux concepts :
  - obligation de proportionnalité des données collectées ;
  - consécration d'un droit à l'oubli numérique et d'un droit à l'effacement des données personnelles ;

- systématisation et généralisation de « l'opt-in » (consentement préalable), notamment en ce qui concerne les cookies, la géo localisation et le commerce électronique ;
- pouvoir autonome de sanctions pécuniaires de la Cnil (1 million d'euros maximum ou 2% du CA mondial de l'entreprise) et durcissement des contrôles ;
- obligation de désignation d'un Correspondant Informatique et Libertés (**CIL**) pour les entreprises employant plus de 250 personnes, dont la mise en œuvre pose quelques difficultés.

⇨ **De nouvelles obligations pour les entreprises :**

- réalisation d'une étude d'impact sur le traitement des données à risques ;
- notification obligatoire des failles de sécurité ;
- encadrement des mécanismes assurant les transferts de données en dehors de l'UE ;
- coopération avec l'autorité de contrôle ;
- instauration d'un principe général de transparence dans le traitement des données qui incombe au responsable du traitement.

⇨ **Ce qui change pour le sous-traitant :**

- précisions sur le rôle du sous-traitant : Création du statut légal du sous-traitant, dont les rapports avec le responsable du traitement doivent être régis par un contrat ;
- partage des missions avec le responsable du traitement.

⇨ **Une réforme nationale est également prévue pour 2014.**

Le Gouvernement français a d'ores et déjà prévu une réforme de la loi informatique et libertés de 1978 sur les données personnelles. Ce projet devrait prendre forme en même temps que le règlement européen mais serait applicable dès fin 2014.
Idéalement : ce texte devrait être une loi de complément régissant notamment la partie pénale (sanctions et peines des manquements) non prévue par le projet de règlement européen.

Les moyens de prévention

On peut recommander aux DSI 4 conseils de base :

- l'instauration et l'actualisation permanente d'une charte d'utilisation de l'outil informatique devant être opposable à tout salarié de l'entreprise ;
- une contractualisation *« sans failles »* de la délégation de pouvoir ;
- l'appel à des compétences externes : juristes, actions de formation ;
- la mise œuvre de la fonction CIL sachant les difficultés que pose l'intégration de cette fonction.

Présentation de l'orateur

André Meillassoux, Ambassade de France à Moscou, coopérant 1982-83. Université de Paris II (3ème cycle de droit international) & Université de Paris IV- Sorbonne (littérature russe), 1981, Institut de Droit Comparé de Paris (IDC) & Diplôme de Traducteur Juridique anglais de l'IDC,1979.

Avocat au barreau de Paris depuis 1983, Associé ATM AVOCATS, 2008, ameillassoux@atmavocats.com.

Président, AFDIT (Association Française de Droit de l'Informatique et de la Télécommunication) 2009-2012, puis 2013-2016, Président, IFCLA (International Federation of Computer Law Associations) 2006-2008, Local representative for France at ITECHLAW (International Technology Law Association).