Le dossier numérique partagé

Dans le cadre des rencontres « Autour d'un verre » d'ADELI

Rapporté par Martine Otter

Une nouvelle rencontre nous a rassemblés le lundi 16 octobre 2006, sur le thème du « Dossier numérique partagé ». Philippe Blot-Lefevre en assurait l'animation.

Le conférencier

Philippe Blot-Lefevre est Fondateur et Managing Director de Hub2b, société spécialisée dans la gestion des risques liés au traitement de l'information et dont le métier se situe à la jonction du droit et de l'informatique qu'il appelle le « DLM », pour « Digital Legal Management ». Philippe Blot-Lefevre est l'auteur d'un ouvrage « Code de confiance »™ à paraître prochainement et qui est consacré à la labellisation d'applications informatiques plus organisées autour de la confiance que de la seule sécurité. Lors de la table ronde qui avait conclu notre Assemblée Générale 2005, Philippe nous avait déjà fait part de ses réflexions et travaux sur le droit d'usage de l'information (qu'il ne faut pas confondre avec celui du SI). Il développe ce thème plus largement à l'occasion de cette rencontre.

Le thème de la confiance

Philippe nous rappela en introduction que :

- « l'information tient sa valeur de son usage. Lorsqu'on protège l'information par les droits d'accès, plus le contenu a de valeur, moins il est accessible. C'est le raisonnement par l'absurde que subissent les applications de dématérialisation !
- Les nouvelles technologies et la mondialisation ont certes beaucoup changé les méthodes de travail, mais les obligations juridiques n'ont pas diminué : elles ont augmenté et apporté leur lot de risques nouveaux.
- Par ailleurs, l'organisation hiérarchique n'est pas adaptée à la gestion des documents, dossiers et autres actifs numériques qui circulent notamment dans les groupes de travail (horizontaux).
- Enfin, sur le plan technique, les outils, en nombre et qualité suffisants, sont exploités à des fins sécuritaires au lieu de suivre les principes juridiques qui servent ces relations interpersonnelles que sont l'information ou son omission, le secret professionnel et la propriété intellectuelle.»

Bref historique

Philippe nous présenta un bref historique de l'histoire de la protection de l'information, en distinguant plusieurs grandes périodes :

- La première, celle de l'ère des moines copistes, où la copie à l'identique est un ascenseur social et le nombre d'exemplaires très limité ;
- La seconde, celle de Gutenberg associée à l'apparition du protestantisme ; le nombre de bibles est multiplié par 250.000 en 50 ans. L'interdiction de copier apparaît alors avec la propriété intellectuelle : il suffit d'ajouter des commentaires personnels au texte initial pour se l'approprier.
- La troisième ère est celle de la ronéo et de la photocopie, qui rend la reproduction de plus en plus facile mais où la diffusion reste complexe.
- Enfin, la période actuelle, celle de l'informatique et de la numérisation généralisée des documents, où la reproduction consiste en un véritable clonage et où les problèmes de diffusion ont disparu.

Ce mode de diffusion instantané ouvre une nouvelle phase des échanges et génère un problème de confiance entre les acteurs en présence. Des actifs et des informations secrètes peuvent facilement être diffusées par erreur et republiées dès lors qu'aucun droit d'usage de l'information diffusée n'est spécifié. Quelques bourdes de ce type sont restées célèbres…

Droit d'accès et droit d'usage

Prenons l'exemple du logo d'une entreprise, accessible sur de multiples supports papier et sur Internet. Quel usage ai-je le droit d'en faire ? L'accès au logo est en principe seulement un droit de voir. Vous n'avez pas le droit de l'utiliser.
On comprend ici la différence entre droit d'accès et droit d'usage : recevoir une information ne vous autorise pas forcément à la republier !
Des règles du jeu sont indispensables, à l'intérieur d'une communauté d'intérêts, pour que l'échange d'informations se fasse dans un cadre de confiance.

Un point important est précisé par l'orateur : la notion d'individu ne compte pas dans la vie professionnelle, en matière d'habilitation d'accès aux informations, tout au moins. C'est notre responsabilité professionnelle qui doit être seule prise en compte dans ce domaine.
Cette notion d'habilitation est essentielle mais encore peu gérée dans les annuaires. Accorder des habilitations à quelqu'un uniquement sur la base de sa fonction, son profil, et pas sur celle de son identité, suppose la mise en place d'un « provisionnement » qui permette d'établir ce lien au travers d'un annuaire.
Cela consiste à relier directement le droit d'usage d'un individu avec son profil.

Illustration pratique de cette répartition des droits : un ingénieur crée une formule chimique, c'est son patron qui seul peut décider de la diffusion de la formule mais n'aura pas le droit de la modifier. L'ingénieur crée et modifie, mais ne décide pas de la diffusion.
Dans cet exemple, une personne crée l'information, une autre décide à qui elle est diffusée

De fait, les organisations sont de moins en moins hiérarchiques, et fonctionnent en groupes de travail. Comment faire dans ce type d'organisation pour que l'information circule en restant protégée ?
Comment gérer des droits d'usage de façon autoritaire ? Cela suppose un consentement des acteurs en présence. Comment faire pour l'obtenir ? Telle est la question posée par Philippe, qui a, bien sûr, une réponse à nous proposer.

Solution : le code de la route

« Notre confiance dans la circulation routière ne tient pas tant à la sécurité technique des véhicules qu'au code de la route dont la signalétique exprime des obligations qui sont respectées dans le monde entier. »
En matière de sécurité de l'information, Philippe Blot-Lefevre propose la mise en place du même type de dispositif, fondant la confiance sur le respect accepté de règles du jeu.
Aujourd'hui, la sécurité « c'est fermer les robinets ». Philippe suggère une logique inverse qui consiste à mettre en place un véritable code pour échanger les informations.
Deux démarches complémentaires sont nécessaires : la mise en place du code lui-même, et une labellisation du système d'information qui permet de respecter effectivement ce code.

Le code

Beaucoup de logiciels utilisent des pictogrammes semblables pour donner des indications qui, d'un éditeur à l'autre sont parfois contradictoires pour l'utilisateur. Philippe a entamé auprès du CEN (Commission de normalisation européenne) et de l'AFNOR une démarche de normalisation consistant à spécifier une dizaine de « signaux » aux significations précises. Ainsi un sens interdit sur fond rouge pourrait interdire toute rediffusion d'un document, un sens interdit sur fond bleu toute rediffusion en dehors de l'entreprise, une imprimante signalerait l'autorisation d'imprimer, etc. Ces signaux sont à définir précisément, mais leur nombre devrait rester limité, pas plus d'une dizaine dans l'esprit de Philippe.

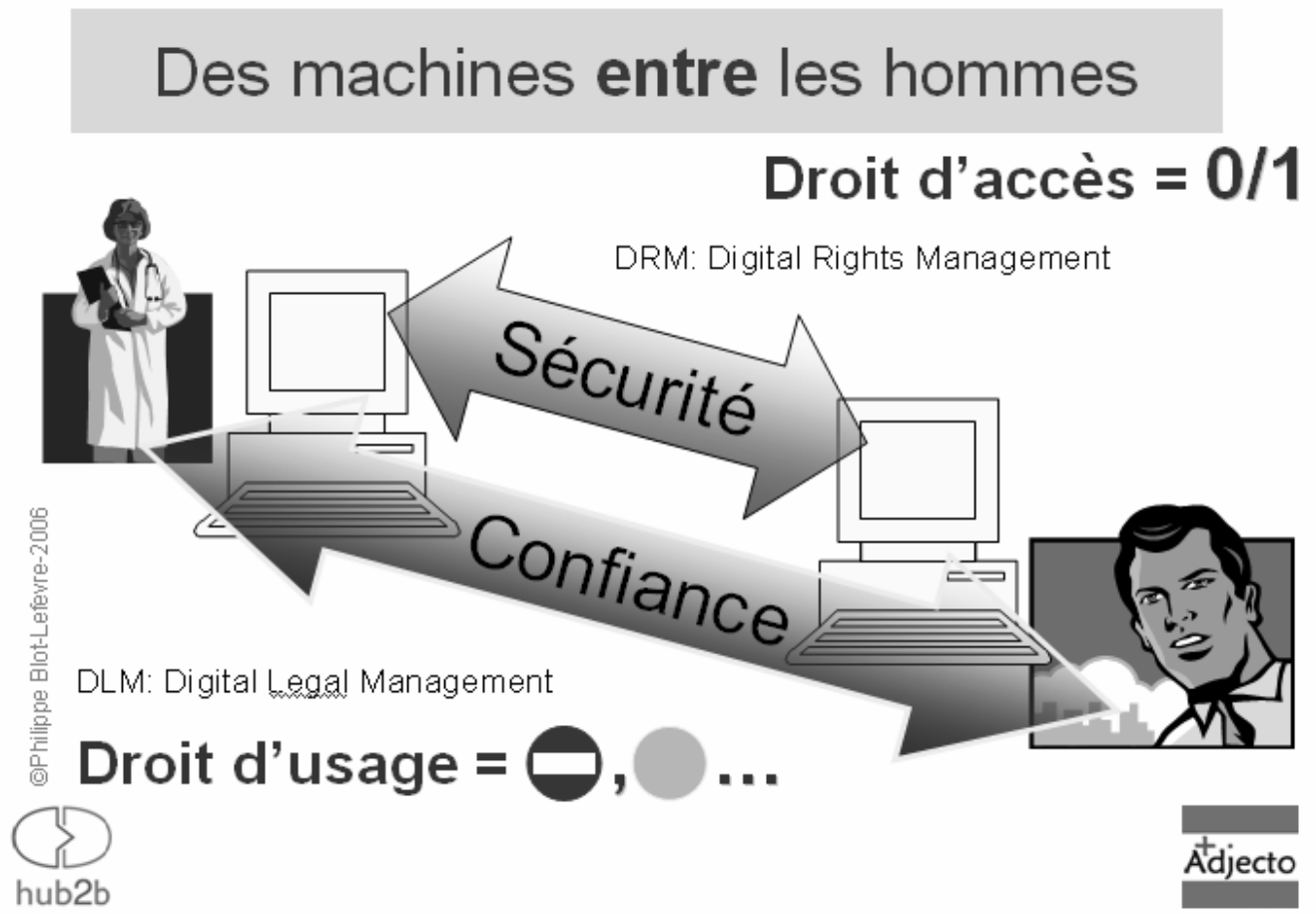
La labellisation

La démarche de labellisation est le volet complémentaire du code de la route. Comme il est impossible de faire respecter le code par tous les acteurs du monde économique, la labellisation vient jouer le rôle du permis de conduire, vérifié régulièrement par une société d'audit indépendante. Un brevet a été déposé sur ce principe par Philippe Blot-Lefevre en 2000, et permet ainsi d'assurer la complétude techno-juridique du dispositif de respect du droit d'usage.
Ainsi 3 sociétés voulant travailler ensemble, auront intérêt à se labelliser, plutôt que de réaliser des audits croisés multiples.
De façon encore plus ambitieuse, un dispositif de certification sous contrôle d'un organisme officiel, national ou international, pourrait être envisagé.

Quelques questions

Pourquoi la question de la sécurité des échanges se pose-t-elle pour Internet ?

La question de la fiabilité des échanges est une question universelle sur le fond, amplifiée par la technologie qui a l'habitude de faire appel à la sécurité pour fiabiliser ses systèmes. Quoi de plus normal ? Mais avec les nouvelles technologies, le problème se pose différemment car les échanges ont lieu entre des individus qui utilisent des systèmes, et pas entre applications comme c'est par exemple le cas de l'EDI. La sécurité est un système inter-technique. Par exemple, l'airbag empêche la tête de cogner le pare-brise ; le firewall empêche les attaques extérieures du Système d'Information. Lorsque des professionnels veulent partager un dossier dématérialisé, la confiance est nécessaire. Les relations interpersonnelles se réglant par le droit (la politesse est une forme de droit parmi bien d'autres), il est nécessaire à ces professionnels de s'entendre sur une règle du jeu avant de collaborer, exactement de la même manière que les automobilistes s'entendent *a priori* sur un sens et un côté de circulation sur la voie publique. C'est bien cette convention « *a priori* » et dûment indiquée qui fait que nous osons prendre le volant pour aller taper quelques balles sur le golf d'Edimbourg ! Il faut la même chose pour les dossiers numériques partagés.
Les débuts d'Internet ont pu se contenter de la Netétiquette parce que la toile était partagée par des chercheurs qui se connaissaient bien mais l'ouverture du système au monde lui a fait perdre toute force. Tout comme la politesse a trouvé ses limites entre les automobilistes qui ont dû adopter un code de la route.



La puissance de la technologie pose un problème : un simple clic peut produire beaucoup de dégâts.
Il faut de plus prendre en compte l'aspect temporel des échanges d'information : comment être sûr de ce qu'il adviendra dans 5 ans à une information archivée ? Qui en sera responsable ?
C'est pourquoi les droits associés aux informations doivent être associés à des profils d'utilisateurs plutôt qu'à des personnes physiques. Ce n'est pas M.X qui a le droit d'accès à telle ou telle information, mais M.X parce qu'il occupe une fonction qui lui confère ce droit.
La logique d'accès varie d'une entreprise à une autre ; Philippe appelle ce traitement le « provisionnement horizontal » et aussi dans la dimension temporelle ; il appelle cela le « provisionnement vertical ».

Nécessité d'une autorité

La mise en œuvre de la confiance est difficile. Depuis 20 ans certains s'emploient à diffuser des méthodes d'analyse de risques et à sensibiliser les directions d'entreprises. Le droit d'usage et son respect ne peuvent se mettre en place sans un minimum d'autorité.
Philippe nous confirme effectivement que la cible de son ouvrage, c'est la Direction Générale. Il s'agit de responsabiliser les hiérarchies, de leur faire prendre conscience des risques encourus par la dispersion anarchique des actifs et des contenus numériques.
Chefs d'entreprise et collaborateurs peuvent se voir condamnés devant les tribunaux ou plus simplement par le marché, voire par leurs partenaires devenus méfiants, pour non respect de cette dispersion.
Ce risque est d'autant plus important qu'aujourd'hui, de plus en plus de transactions de contenus passent par Internet de façon non-sécurisée. Et comme les gouvernements ne savent pas comment endiguer l'hémorragie des données sensibles, l'inflation galopante de la réglementation menace sévèrement le personnel et son management

L'usage de l'e-mail

La question de la valeur d'usage de l'e-mail apparaît naturellement au cœur du débat : comment contrôler sa réutilisation éventuelle par le destinataire ? Et cela fait, comment s'assurer de la non-répudiation des éléments qui caractérisent la correspondance : l'identité de l'émetteur et du destinataire, la réception, la prise de connaissance ?

Témoignage d'un avocat :
« La correspondance entre confrères devrait être protégée, mais tous les avocats échangent des informations avec leurs clients via internet. L'aspect immédiat et confortable d'internet pousse à ne pas se protéger. »

Dans un e-mail l'identité de l'émetteur et du récepteur sont difficilement vérifiables.

Un élément juridique essentiel est précisé : certains échanges d'information s'inscrivent dans un rapport de droit préexistant, qui précise souvent des clauses de confidentialité, par exemple entre un employeur et un salarié, un client et un fournisseur. Le besoin de limiter le droit d'usage n'apparaît vraiment indispensable que si l'échange d'information ne s'inscrit pas dans un rapport de droit préexistant.

Les clauses diverses de confidentialité, souvent ajoutées à la fin des messages (clause de disclosure) n'ont pas de valeur en droit français, car elles sont non-consenties. On lit souvent : « détruisez ce massage si vous n'êtes pas le bon destinataire », cela est d'autant plus stupide que cet avertissement apparaît à la fin du message et pas au début…

Proposition d'un espace de confiance

Face à la tâche gigantesque de sécurisation d'un échange de contenu, la solution « code2confiance», proposée par Philippe Blot-Lefevre s'apparente à l'adhésion à un contrat commun entre les personnes amenées à échanger des informations.

Dans un cadre professionnel le nombre de type de destinataires et type de documents échangés peut être assez restreint. D'expérience, les règles définissant les droits d'usage, une fois définies pour ces différentes cibles, restent généralement assez stables et limitées.

Un autre aspect difficile à résoudre est celui de la mise à jour des informations transmises, qui pose la question de la non répudiation : comment faire en sorte qu'un tiers ne puisse pas prétendre « qu'il ne savait pas » ? Par exemple dans le cas d'une mise à jour de tarif : un fabricant change ses tarifs. Son distributeur assure qu'il ne les a pas reçus. Comment savoir alors qui dit la vérité ? Il faut disposer d'un jeu de traces et de notifications permettant de prouver que l'information a bien été reçue, envoyée ou oubliée ; l'omission étant souvent aussi engageante que l'action !

Nécessité de l'éducation

Le respect de la loi ne va pas toujours de soi dans notre culture latine. Un système d'éducation est nécessaire mais devrait rester simple si on se limite à 10 signaux.
Philippe indique que, dès à présent, la Chambre de commerce chinoise est intéressée par ce dispositif de droit d'usage et commencerait à prendre conscience de la nécessité, si l'on veut continuer à travailler ensemble utilement, de respecter les droits de propriétés intellectuelles, dans un contexte d'échanges internationaux et ciblés.

Application côté grand public ?

Le principe du droit d'usage serait-il également utilisable en dehors du monde de l'entreprise ? Et apporterait-il une solution aux échanges peer to peer ?

Pourquoi pas ? Philippe indique que l'on pourrait tout à fait imaginer que des supports multimédia soient commercialisés avec 2 prix de vente différents, l'un au prix fort de 40 euros non-copiable avec un cd protégé par un anti copie et l'autre, à prix réduit de 5 euros, avec un engagement de ne pas recopier et une amende dissuasive en cas de non-respect de l'engagement pris. Une future loi pour la protection des œuvres musicales pourrait prévoir un dispositif de ce type.

À la question de la nature de la sanction à appliquer suivant le pays, Philippe répondit qu'elle pourrait être dans chaque cas fixée suivant le droit local…

La question de l'intimité et de la protection des données personnelles dépasse également les frontières de l'entreprise.

En matière de Dossier Médical, la confiance n'est pas toujours au rendez-vous : on a pu citer le cas de patient cancéreux ne se faisant pas rembourser ses médicaments par crainte d'une fuite pouvant porter atteinte à sa notoriété. Une labellisation des organismes ou administrations pourrait répondre à ce besoin de confiance.

La classification des informations est-elle incontournable ?

Le droit d'usage permettrait-il d'échapper à la classification systématique des informations, telle que la recommande l'ISO 27001[1] ? Il s'agit en effet d'un travail épouvantable, véritable tonneau des Danaïdes.

Oui et non, répond Philippe, le droit d'usage peut être attribué à la volée, lors de la diffusion de l'information, sans classification préalable. Mais il faut quand même décider d'une typologie générale des documents et des profils et décider d'un annuaire d'habilitations suivant les fonctions.

Conclusion

Les participants ont été dans l'ensemble séduits par l'idée d'une signalétique comprise par les utilisateurs, qui dépasserait la barrière des langues. Le droit d'usage, souligne une participante, est une méta donnée attachée au document. Et citant Jean Denègre, « les méta données sont aux données ce

1 ISO/IEC 27001:2005 "Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences" (disponible seulement en anglais)

que l'étiquette est au médicament », elle suggère de rendre la méta donnée « droit d'usage » obligatoire. L'intérêt principal souligné est de trouver une solution de communication à l'intérieur de groupes fermés d'intérêt, face aux limites de la combinatoire de l'analyse des risques.

Nous ne pouvons qu'applaudir à cette initiative de mise en œuvre d'une logique de confiance en lieu et place de celle d'une logique de défiance.

Prochaine étape : la parution du livre de Philippe, et d'autres article dans la Lettre d'ADELI… ▲

martine.otter@adeli.org

Contact

Philippe Blot Lefevre
63, rue de Boulainvilliers
75016 Paris
philippe.adeli@code2confiance.org
Mobile : 06 07 54 32 07