Chapitre 6

Les risques de l'offshore

Les sociétés qui envisagent de confier certaines de leurs réalisations en offshore associent presque toujours cette initiative à un risque important et mal maîtrisé. Il convient cependant de relativiser les risques attribués aux développements en offshore car nombre d'entre eux sont aussi élevés, voire davantage, lorsque les développements sont réalisés localement, au sein même de la société, à l'exemple du risque que des créations originales soient divulguées à la concurrence.

De nombreux clients de l'offshore présupposent que certains sujets sont particulièrement exposés. Une crainte fort répandue est que le prestataire en offshore ne détourne le code qui lui est confié pour créer un produit concurrent ou le revendre. D'autres craintes concernent la sécurité des communications entre sites ou le montant des marges prélevées par le prestataire.

Force est pourtant de constater que le plus grand risque qui menace un projet en offshore est que le client ne sache pas le gérer à distance. Nombreux sont en effet les projets que les clients se révèlent incapables de gérer, tout en reportant la responsabilité de l'échec sur leur prestataire. Pour ce dernier, le risque principal est que le client ne paye pas, et chaque nouveau client est pour lui une source d'inquiétude.

Le partenaire

Lorsqu'on choisit de travailler avec un prestataire en offshore, il est essentiel de savoir à qui l'on a affaire. Le client se trouve démuni pour juger du sérieux de son partenaire. Certains prestataires n'ont pas même d'existence légale, en dépit de la qualité professionnelle de leurs sites Internet, de leurs nombreuses références et du grand nombre de personnels qu'ils emploient.

Pour se prémunir des conséquences notamment juridiques de telles collaborations, il est courant de demander au prestataire de communiquer ses statuts, si possible traduits en anglais. On peut ainsi connaître la nature de la société ainsi que l'identité des associés.

La structure de l'actionnariat est importante pour comprendre le type de société auquel on a affaire. Si l'on découvre que la société du prestataire est en fait une fi liale d'un éditeur de logiciel américain, on prendra soin de s'assurer que l'activité de développement que

l'on en attend sera gérée avec tout le sérieux nécessaire. Si la société est la filiale, peut-être récente, d'un grand prestataire indien, on se demandera quel sera l'impact du projet qu'on souhaite lui confier sur la stratégie de ce prestataire. On peut aussi légitimement redouter que la société ne soit liée à un concurrent.

L'existence de références parfois remarquables n'est pas un gage que la société est juridiquement constituée. Les clients précédents n'ont peut-être pas pensé à vérifier son statut ou ne s'en sont pas préoccupés. Il vaut toujours mieux vérifier cette situation par soi-même.

> **EN RÉSUMÉ**
> **Statut du partenaire**
> Il est important de bien connaître son partenaire. Il est recommandé pour cela d'exiger les statuts de la société en offshore et de les faire traduire avant de prendre sa décision. Il est important que le prestataire ait une existence légale.

Les litiges en offshore

Lorsque des tensions surgissent avec le partenaire en offshore, il ne faut pas hésiter à rechercher un médiateur susceptible d'aider les parties à trouver une solution à l'amiable au lieu de laisser la situation se dégrader. Il peut être utile de prévoir une telle clause dans les contrats qui lient le client au prestataire, car ces médiateurs donnent généralement d'excellents résultats.

En cas de litige, le client peut avoir un contrat-cadre avec un cabinet d'avocats, lui permettant de consommer un certain volume d'heures d'avocat (*retainer*). Cela rend le coût de gestion du litige pratiquement nul. Même s'il doit payer un cabinet d'avocats pour ses prestations, le client utilisera son cabinet habituel, dont il contrôle assez bien les coûts.

Pour le prestataire, la situation est tout autre. Il doit prendre un avocat dans un pays distant qu'il connaît mal, aux tarifs très élevés en comparaison de ceux en vigueur dans son pays. La gestion du litige s'accompagne de surcroît de voyages et de séjours à l'hôtel, qui en alourdissent encore le coût. Dans ces conditions, seul un litige réellement important peut justifier de telles dépenses par le prestataire pour se défendre ou attaquer.

Les décisions des tribunaux dans le pays du client ne sont pas toujours faciles à faire appliquer dans les pays de l'offshore, surtout s'il s'agit de sommes modiques ou de restitution de code source. Bien que théoriquement applicables dans les pays de l'offshore, les condamnations sont rarement exécutées dans la réalité. Par exemple, les procès intentés par les grands éditeurs pour la protection des licences ont porté peu de fruits. La faible volonté des juridictions des pays de l'offshore d'exécuter les condamnations est parfois amplifiée par la perception que la décision est injuste puisque le prestataire n'a pu défendre ses chances à armes égales.

Pour éviter de telles situations, le client peut avoir intérêt à prendre un excellent avocat du pays de l'offshore. Les décisions de justice éventuelles sont alors beaucoup plus faciles à faire appliquer. Les coûts des avocats sont par ailleurs modiques dans certains pays d'offshore, et il est possible d'être correctement représenté.

Protection de la propriété intellectuelle

La première préoccupation d'un chef d'entreprise ou d'un responsable du développement concerne la propriété intellectuelle qui est transférée en offshore et tout particulièrement les codes source. On associe assez naturellement la valeur d'un développement à son code source, et l'on souhaite le protéger au mieux.

La crainte que les sources qui ont servi à réaliser le projet soient détournés par le prestataire ou un de ses collaborateurs n'est pas sans fondement. Quand on voit comment les lois sur les copyrights sont ouvertement ignorées dans les pays de l'offshore, on a tout lieu de redouter que les produits du client soient détournés. Même si on ne sait pas exactement ce qui pourrait arriver au code source, on panique à l'idée de le retrouver sur un autre marché géographique ou de voir le prestataire le revendre à des concurrents.

Si le risque de détournement de la propriété intellectuelle existe bel et bien, il est rare qu'il se concrétise à des fins commerciales. Les prestataires en offshore opèrent dans des zones où, bien souvent, il n'existe pas de réel marché local du logiciel, rendant l'exploitation de tels détournements peu rentable et fortement risquée. Les produits de grande diffusion commercialisés sur Internet sont beaucoup plus exposés car la fraude peut être initialisée par une seule personne indélicate et mener à des profits certes faibles, mais rapidement acquis.

C'est finalement en terme de réutilisation sur d'autres projets que le risque est le plus important, d'autant que les informaticiens qui réutilisent un code qu'ils ont un jour créé y perçoivent avant tout un gain de temps et n'y voient pas forcément malice.

Propriété du code source

Il existe de fait un risque juridique sur la propriété du code source. Dans la plupart des pays, le payeur n'est pas nécessairement le propriétaire du code source, car c'est le créateur du code qui en est le propriétaire naturel.

Certains prestataires en offshore mettent clairement en avant leur désir de construire des offres de produits à partir des réalisations qui leur sont confiées. Ils font valoir qu'ils sont les propriétaires du code source, dont ils accordent une licence éternelle au client payeur. Parfois, le prestataire revend des services sur la base d'un développement réalisé pour un premier client. Celui-ci, payant pour un plein développement, peut accepter que le prestataire réutilise le cœur du développement pour construire d'autres solutions. Gagnant ainsi du temps, le prestataire reverse alors des droits au client pour avoir utilisé du code développé initialement pour lui.

De tels arrangements ne peuvent se produire que si le prestataire agit en tant qu'utilisateur final ayant un besoin d'exploitation et qu'il n'envisage pas de revendre le logiciel. Par exemple, un client industriel qui met au point une gestion de stock s'appuyant sur un ERP du marché peut ne pas s'opposer à ce que son prestataire essaie de packager le produit et de le revendre, pour peu que le coût du projet s'en trouve diminué. Ce client n'étant pas un éditeur de logiciel, il souhaite avant tout optimiser les coûts de ses réalisations.

Pour la plupart des clients de l'offshore, cette situation est toutefois inacceptable. Ils veulent avant tout utiliser les forces de production en offshore pour créer leurs produits

dans les meilleures conditions possible. À leurs yeux, le prestataire ne doit avoir aucun droit sur les réalisations en offshore, tout particulièrement s'ils sont éditeurs de logiciels.

En réalité, ce sont les clauses du contrat qui déterminent qui est le propriétaire de la création intellectuelle. Comme nous le verrons au chapitre 9, consacré au contrat avec le partenaire, le contrat doit clairement préciser que la propriété intellectuelle de toutes les créations en offshore, incluant le code source et tous les éléments créés ou échangés au cours du projet, revient au client et que le prestataire n'a aucun droit sur elles.

Une règle claire consiste à imposer que les productions réalisées dans le cadre du projet (code source, notes, spécifications, etc.) portent la mention *Copyright… Client… Année…* Cela permet non seulement de marquer les documents comme protégés, mais aussi de faire la preuve au besoin que les collaborateurs en ont été pleinement informés.

EN RÉSUMÉ

Propriété du code source

La propriété du code source comme de toute création réalisée chez un prestataire en offshore doit être clairement attribuée par contrat au client. En effet, le payeur des prestations n'est pas nécessairement le propriétaire juridique de la création.

Rétention des sources en offshore

La situation devient rapidement délicate lorsqu'un conflit se développe entre le client et le prestataire. Si les paiements ne sont pas effectués comme ils le devraient, le prestataire offshore commence le plus souvent par bloquer la livraison du code source, si c'est techniquement réalisable. Si le client n'a pas honoré ses factures par négligence ou du fait de difficultés passagères, l'effet de ce bras de levier est désastreux. Le client ressent toute la puissance de la rétention du code source, se sent pris en otage et perd rapidement confiance dans le prestataire.

Quelle que soit la situation concrète, le prestataire n'a guère que deux moyens de pression sur le client : la rétention du code source et la dissolution de l'équipe de développement. Cette dernière, lorsqu'elle va au-delà de la simple menace, est le plus souvent la marque d'une volonté de mettre fin à la relation commerciale plutôt que de rechercher un accord. La rétention du code source et des livrables est donc la seule arme réelle en possession du prestataire s'il souhaite poursuivre la collaboration.

Le fait d'avoir exprimé dans un contrat que le prestataire n'a aucun droit à exercer une rétention des livraisons n'est guère dissuasif dès lors que le prestataire considère que le client ne respecte pas ses propres engagements et que la situation est déjà conflictuelle.

La tension a toutes les chances de monter d'un cran si le client s'imagine que le prestataire va utiliser le produit qu'il garde en otage à son propre profit. Il s'agirait en ce cas non plus d'un moyen de pression, mais d'un acte délictueux, mettant potentiellement en danger l'activité de la société cliente. Ce risque n'est pas une vue de l'esprit, et il arrive que de petits prestataires qui n'ont pas été payés considèrent unilatéralement que le produit du client leur échoit en dédommagement des impayés.

EN RÉSUMÉ

Rétention des sources comme moyen de pression

Un prestataire en offshore utilise volontiers la rétention des codes source comme moyen de pression sur son client en cas de conflit. Les protections contractuelles sont sans effet pour interdire au prestataire de retenir les livrables.

Faire appel à un médiateur est un signe fort de recherche de conciliation. Lorsqu'un client traite avec un représentant local de l'offshore — comme expliqué au chapitre 2, certains prestataires disposent d'un agent commercial dans le pays du client —, ce dernier joue naturellement un rôle de médiateur, pour peu qu'il ne soit pas lui-même impliqué dans le conflit. Le recours à un médiateur est abordé au chapitre 9.

La meilleure solution pour se protéger du blocage des livrables est de mettre en place un référentiel dans lequel toute la production est déposée au fur et à mesure de sa création. Le référentiel du prestataire est synchronisé en temps réel, ou presque, avec celui du client. Dès lors, le prestataire ne peut exercer de chantage sur la production réalisée, et le blocage des livrables ne peut concerner que la production à venir, ce qui est beaucoup moins grave.

Cette synchronisation en continu est très importante en offshore, et ce, à plusieurs titres. Le fait de demander explicitement la livraison du code source est toujours perçu comme une attitude agressive. Le prestataire se demande pourquoi son client le lui demande. Au mieux, il s'imagine que le client effectue une revue de code ou critique l'organisation des sources. Il suppose peut-être aussi que le client veut interrompre la collaboration et récupérer ce qui lui est dû avant de l'annoncer au prestataire. Si la demande de livraison du code source est faite en situation de conflit, il y a toutes les chances que le prestataire la prenne comme une déclaration de guerre et qu'il ne livre pas les éléments demandés.

> **EN RÉSUMÉ**
>
> **Protéger les sources par une synchronisation permanente**
>
> Pour éviter que le prestataire exerce une pression sur le client en bloquant les livrables, il est recommandé d'organiser une gestion de référentiel obligeant le prestataire à y placer régulièrement tous les éléments de la production. Le référentiel est synchronisé en temps réel ou quotidiennement avec le référentiel chez le client, engendrant une livraison continue de la production. Le blocage des livraisons par le prestataire ne peut dès lors concerner que le futur, ce qui est moins contraignant pour le client.

Arrêt des prestations en situation de conflit

Lorsque les prestations s'interrompent du fait d'un conflit, des règlements peuvent être dus au prestataire alors que les livrables ont été remis au client dans leur intégralité. Indépendamment des responsabilités de chacun dans la rupture, le prestataire considère en ce cas qu'il est en droit de récupérer son dû sur les actifs dont il dispose, y compris le code source.

De son côté, le client peut estimer avoir perdu beaucoup plus que la somme restant due au prestataire. L'absence des dernières livraisons et les retards sur la production peuvent représenter pour lui des montants très importants. Il peut même envisager de poursuivre le prestataire pour le préjudice et les dommages qu'il a subis.

Nombre de prestataires n'hésitent pas, en compensation de la dette du client, à tenter de vendre le produit à leur compte ou à réutiliser le code source pour leurs propres développements. Le seul moyen pour un client d'empêcher un prestataire de le faire est de négocier avec lui, non seulement en raison de l'aléa judiciaire, mais parce que les décisions de justice ne sont pas toujours appliquées, d'autant plus dans les pays de l'offshore.

EN RÉSUMÉ

Une fin conflictuelle

Lorsque les prestations se terminent en situation de conflit et que des sommes restent dues au prestataire, ce dernier considère le plus souvent qu'il peut disposer à son gré du produit développé pour son client. Il est toujours préférable de privilégier la négociation plutôt que la rupture.

ÉTUDE DE CAS

Déliquescence du partenariat

Un éditeur américain utilise des ressources en offshore pour réaliser des produits très spécialisés concernant l'analyse de données d'une production pétrolière. Peu confiant par nature, il se méfie des prestataires en place et monte sa propre équipe dans un joint-venture. Il embauche pour cela un manager de sa connaissance dans le pays.

Le projet démarre bien, et les premiers projets sont satisfaisants. Bientôt, la société aux États-Unis connaît des difficultés, et ses revenus se font erratiques. Sans visibilité, l'éditeur cesse ses paiements au joint-venture en offshore sans donner d'explications. Les mois passant, le manager de la structure offshore exige d'être payé.

Après six mois sans paiement ni explications, le manager passe à l'action et entre en contact avec des clients de l'éditeur auxquels il explique sa situation, à son avantage bien sûr. Il explique qu'il est désormais propriétaire du produit et qu'il en assurera dorénavant la maintenance à 30 % du prix pratiqué par l'éditeur américain.

Les clients contactent immédiatement l'éditeur américain. Ce dernier se veut rassurant, mais le mal est fait. L'éditeur tente de régler le problème en cherchant à négocier avec le manager en offshore. Il constate alors que son joint-venture n'existe plus et que le manager opère à partir d'une société qu'il a créée pour ce produit.

Le manager a contacté tous les clients de l'éditeur qu'il connaissait afin de leur proposer d'acquérir le produit à travers lui. L'éditeur américain menace de poursuivre son ancien manager et ceux qui se sont associés à lui, arguant du fait que les lois du pays de l'offshore sont intraitables quant au respect de la propriété intellectuelle.

Essuyant un refus de la part de tous les clients contactés, le manager disparaît finalement, et les choses en restent là, fort heureusement pour l'éditeur américain. Ce dernier mettra cependant un temps considérable à redorer son blason, sans parvenir à rétablir tout à fait sa crédibilité.

Utilisation de bibliothèques de programmes

Outre le risque de détournement de la propriété intellectuelle du code source, il convient de s'attacher à protéger ce dernier contre l'inclusion de sections de code qui seraient la propriété de tiers.

Il peut être tentant pour les développeurs en offshore d'employer des portions de code « empruntées » à des tiers plutôt que de les développer eux-mêmes. Pour gagner du temps ou parer au plus vite à leurs insuffisances, ils peuvent employer du code qu'ils pensent libre car provenant de projets Open Source aussi bien que du code source commercial.

Ce risque est plus courant qu'il n'y paraît. Par exemple, un développeur qui travaille sur un domaine technique précis a de grandes chances de se voir confier des projets similaires. Très naturellement, parfois sans même penser à mal, il se peut qu'il réemploie du

code du projet précédent. Puisqu'il a un même problème à résoudre, il lui semble naturel d'appliquer une même solution. L'ennui est que ce code source ne lui appartient pas mais appartient au client du projet précédent.

Si même il est conscient du problème, il peut se dire que les deux clients ont peu de chances de découvrir la réutilisation du code. Le problème peut devenir sérieux si le premier client, propriétaire du code, a fait de ces couches techniques un atout concurrentiel qu'il protège autant que possible et qu'il en découvre l'usurpation.

Il se peut aussi que le code réutilisé provienne d'une solution logicielle à licence payante, comme Oracle TopLink ou des parties de BEA WebLogic. Bien évidemment, ces produits sont soumis au paiement de licences, le plus souvent selon l'utilisation que l'on en fait, par processeur. Si l'on ne contrôle pas correctement le code source, on peut découvrir que la solution nécessite des licences payantes pour être déployée.

Il n'est guère possible de se protéger de ce risque par contrat, car si le prestataire utilise un tel code source et qu'il y ait un réel préjudice, il est hautement probable qu'une action en justice condamne ceux qui auraient bénéficié de la fraude, en l'occurrence le client, en même temps que le prestataire. De plus, si le prestataire ne peut honorer les dommages et intérêts exigés, ce qui est plus que probable puisque les sommes en jeu peuvent se révéler très élevées, le client seul solvable se retrouve seul tenu de dédommager la partie lésée.

Pour avoir quelque efficacité, le contrat doit bien sûr interdire explicitement l'utilisation de code source externe sans l'accord explicite du client mais surtout s'accompagner d'un suivi régulier des développeurs, surtout dans les domaines techniques, car ils sont les plus tentés de réutiliser des programmes licenciés. Ajoutons que ces blocs logiciels sont assez faciles à détecter avec des outils d'analyse de code.

> **EN RÉSUMÉ**
>
> **Codes source utilisés frauduleusement**
>
> Le contrat entre le client et le prestataire précise qu'il est interdit au prestataire d'utiliser des codes source qui sont soumis à des droits d'usage ou qui appartiennent à un tiers. Il est fortement recommandé d'assurer un suivi rigoureux de ces règles dans le cours des développements.

Fractionnement du code source

Certains clients, surtout parmi les éditeurs de logiciels, ne veulent pas donner la totalité du code source d'une application à un prestataire de peur qu'il puisse être détourné. Cela limite fortement la nature des projets susceptibles d'être confiés aux équipes en offshore. Ces dernières ne peuvent que travailler sur des modules autour du noyau central ou sur les fondations techniques des applications. Le plus souvent, on leur confie des projets périphériques, ce qui engendre les effets négatifs mentionnés au chapitre précédent.

Les clients qui donnent tout le code source de leur produit au prestataire choisissent parfois de contrôler les accès à chaque module du code par le biais d'un référentiel de façon que personne ne puisse disposer du code source complet. Rien n'empêche cependant les développeurs du prestataire de collationner le code de chaque module afin d'en reconstituer l'intégralité. Si l'intégration et le déploiement sont assurés en offshore, les personnes qui s'occupent de ces tâches ont nécessairement accès à l'ensemble des modules pour pouvoir les compiler et les déployer.

La plupart des clients considèrent que la protection qu'apporte le fractionnement du code source est illusoire et préfèrent faire confiance au prestataire pour atteindre une productivité maximale.

Confidentialité des informations

Il est habituel de demander au prestataire de signer un accord de confidentialité, ou NDA (Non Disclosure Agreement), avec le client. Assez standard, ce type d'accord décrit ce qu'est une information confidentielle et indique le plus souvent que les mêmes protections doivent être portées à ces informations du client qu'aux informations confidentielles du prestataire. Bien souvent, cet accord est signé par le management du prestataire, et les collaborateurs distants n'en sont pas informés.

Il peut être plus judicieux du point de vue psychologique de demander à chaque collaborateur travaillant pour le client de signer l'accord de confidentialité. Dans les pays de l'offshore où l'on ne signe que très peu de documents et où le contrat de travail lui-même n'est pas toujours écrit, le fait d'apposer sa signature à un accord de confidentialité engage réellement. On peut de plus en profiter pour rappeler certaines règles concernant le respect de la protection de la propriété intellectuelle.

> **EN RÉSUMÉ**
> **Accord de confidentialité**
>
> Le client demande à chaque membre de l'équipe en offshore de signer un accord de confidentialité exprimant clairement quelles sont les informations jugées confidentielles et certaines autres règles, notamment sur la protection de la propriété intellectuelle. Cet accord est perçu comme un engagement personnel fort.

Les informations confidentielles

Le prestataire en offshore a forcément accès à un ensemble assez vaste d'informations que le client souhaite protéger. Il peut s'agir de codes source (*voir la section précédente*), de spécifications ou d'informations sur le produit, ses anomalies ou ses faiblesses connues.

Le client souhaite naturellement assurer la protection de ces informations, à commencer par le fait de ne pas les rendre accessibles à tous chez le prestataire offshore, en particulier aux visiteurs. Toutes les informations confidentielles, ou presque, sont rendues disponibles sous forme informatique. Il est important de savoir précisément où se trouvent ces informations et comment elles sont gérées, car, à défaut de protection, elles peuvent être aisément copiées sur n'importe quel poste du réseau local.

Dans les cas où l'on aurait choisi de monter sa propre filiale en offshore ou un joint-venture, les informations sont naturellement isolées. C'est d'ailleurs souvent l'une des raisons qui conduit à monter ce type de société en offshore.

Gestion d'un référentiel

Si l'on souhaite contrôler les informations qui sont rendues disponibles chez le prestataire, la première chose à faire est de mettre en place un référentiel. IBM Rational ClearCase, par exemple, est un excellent outil pour cela. Il possède notamment une option

multisite permettant de synchroniser les référentiels distants. Ses principaux concurrents sont Merant PVCS et Continuus.

Le prestataire doit s'assurer que tous les éléments et informations sont placés dans le référentiel. Chaque élément du référentiel ayant ses propres règles d'accès édictant qui a le droit de voir ou de modifier chaque fichier, on peut savoir qui a extrait un élément, à quel moment et s'il a changé quelque chose.

La figure 6.1 illustre les différents moyens de partager des informations entre un site en offshore et le client. Ces différents moyens de partage d'informations ne sont pas interchangeables. Les référentiels sur un LAN, par exemple, comme ceux que proposent Telelogic ou IBM Rational, offrent la meilleure sécurité, mais à un coût important.

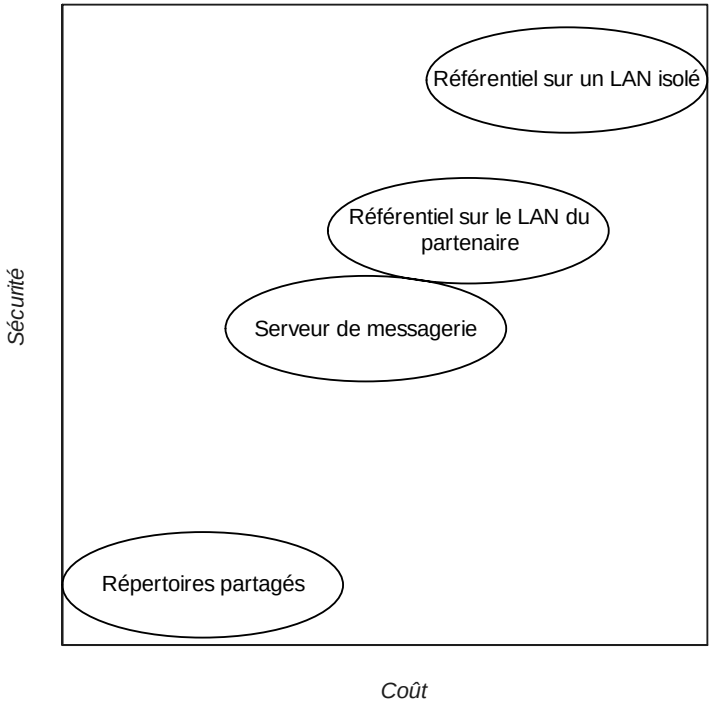

Figure 6.1. Solutions de partage d'information

Les gestionnaires de documentation tels que Microsoft SharePoint peuvent jouer un rôle assez similaire pour rassembler l'information et en protéger l'accès. Les gestionnaires de référentiels tels que ClearCase permettent toutefois de gérer plus efficacement les opérations relatives au développement. On y trouve notamment des fonctionnalités de gestion d'un ensemble de fichiers et de codes source formant une version de référence (*baseline*) et la possibilité d'y associer une gestion du changement permettant de suivre le workflow des corrections d'anomalie et des demandes d'évolution.

Les serveurs de messagerie

Les serveurs de messagerie recueillent eux aussi des informations confidentielles par le biais des messages échangés. Avec des équipes importantes, il est intéressant d'isoler le serveur de messagerie chez le prestataire de sorte à le dédier à l'équipe. Le gain en confidentialité est important.

Si l'on ne met pas en place un serveur de messagerie dédié, le serveur de messagerie commun contient des informations du prestataire, du client et d'autres clients, lesquelles se retrouvent dans les sauvegardes. Le client n'a alors aucun contrôle sur la localisation et la gestion de ces sauvegardes. De plus, les administrateurs du serveur chez le prestataire peuvent ouvrir les comptes des utilisateurs et voir les informations qui y sont placées.

En dédiant un serveur de messagerie, on obtient une confidentialité accrue, et le prestataire peut exiger l'application de procédures strictes pour en assurer l'administration sans risque. Le serveur de messagerie peut aussi garder les traces de tous les messages reçus et envoyés pour analyse en cas de problème. Ces traces sont accessibles à un administrateur de serveur.

Isolement des équipes

Lorsqu'un projet mobilise une équipe importante en offshore, le client peut demander au prestataire d'isoler cette équipe du reste de la société. L'isolement est naturel en cas de création de filiale ou de joint-venture en offshore. Dans les petites équipes, de moins de vingt personnes, l'isolement des équipes et du réseau peut toutefois se révéler trop coûteux en comparaison de la taille des projets.

Par ordre d'importance, il faut isoler le réseau du projet du reste du réseau du partenaire en offshore puis isoler physiquement le lieu où travaillent les collaborateurs du projet. On doit aussi mettre en place les procédures qui assureront l'efficacité de cette séparation (*voir ci-après*).

Isolement du réseau local

L'isolement d'une partie du réseau local du partenaire peut être total ou partiel. On peut, dans un premier temps, mettre en place des serveurs dédiés au client, avec des règles d'isolement et des audits pour vérifier que ces règles sont appliquées. De cette façon, le client peut exercer un contrôle fin sur la gestion des serveurs, les sauvegardes et les droits d'accès.

Ces mesures peuvent toutefois se révéler insuffisantes. Les serveurs, par exemple, sont toujours physiquement accessibles par tous les collaborateurs en offshore. Une personne mal intentionnée pourrait trouver le moyen de les pénétrer afin de récupérer des informations. De plus, le client ignorant comment le réseau est géré, il ne peut être certain qu'un niveau de sécurité suffisant est appliqué.

Le client peut donc souhaiter isoler totalement son réseau local de celui du prestataire. Aucun composant réseau n'est alors partagé, et les utilisateurs du réseau du prestataire ne peuvent accéder physiquement à celui du client. Une telle option a un coût important. Le client doit acheter le matériel réseau (switch, pare-feu, serveurs, système de sauvegarde), les licences (systèmes d'exploitation, serveur de messagerie, logiciel de sauve- garde, etc.) et

la bande passante sur Internet. De plus, le réseau passant sous sa responsabilité, il lui faut certainement embaucher des administrateurs pour le gérer en offshore.

ÉTUDE DE CAS

Non-respect des règles de gestion du réseau local

Une société opte pour la mise en place d'un réseau local dédié. Deux administrateurs réseau font partie de l'équipe du client, elle aussi clairement dédiée, pour gérer les soixante ordinateurs de l'équipe. Le réseau doit être parfaitement isolé, avec des équipements, un serveur de messagerie et une bande passante sur Internet également dédiés. Les règles sont strictes et clairement exprimées par écrit.

Après quatre mois de travail avec ces équipes, on s'aperçoit que la synchronisation du référentiel entre Paris et l'offshore ne fonctionne pas correctement et qu'elle est d'une lenteur intolérable, surtout la nuit.

On dépêche une mission d'audit. Il apparaît que certaines règles ne sont pas respectées. Le responsable de l'informatique interne du prestataire maintient de fait un rôle de supérieur hiérarchique envers les administrateurs qui travaillent dans l'équipe dédiée du client, laquelle lui demande souvent des conseils pour la configuration de certaines machines. Constatant l'énorme quantité de bande passante inutilisée la nuit, ce responsable a mis en place un système autorisant les utilisateurs du réseau du prestataire à accéder à cette bande passante après une certaine heure.

Le prestataire n'imposant pas de règles strictes sur l'emploi d'Internet, un certain nombre d'employés téléchargent toutes les nuits musiques, films et programmes et saturent la bande passante. Il ne reste pratiquement plus rien pour les usages professionnels du client qui souhaite réaliser ses synchronisations de nuit.

Sans audit, il aurait été impossible de détecter ces dysfonctionnements et d'y remédier. Des sondes et des outils recherchant les vulnérabilités ont ensuite été utilisés régulièrement pour détecter ces accès non autorisés.

Le contrôle des accès

Pour s'assurer que les informations sont correctement protégées, on peut organiser l'isolement des équipes en offshore. Elles travaillent en ce cas dans des salles séparées, accessibles uniquement aux membres de l'équipe du client. Pour être efficace, ce système nécessite que l'accès aux locaux soit contrôlé par des cartes personnelles, qui identifient chaque personne entrante et sortante et mémorisent les heures de passage aux portes.

Même si toutes les personnes concernées disposent d'une carte personnelle d'accès dans les locaux, encore faut-il qu'elles ne fassent pas entrer d'autres personnes. Certains systèmes sophistiqués proposent des sas à une personne, qui garantissent des accès physiques individuels. D'autres contrôlent les sens entrée et sortie afin que seules les personnes qui sont effectivement sorties puissent entrer à nouveau, évitant de la sorte le prêt de cartes. Des caméras peuvent être ajoutées au système pour contrôler les entrées-sorties.

Toutes ces règles d'accès ne sont toutefois pas faciles à appliquer, et l'on constate souvent, à l'occasion des fêtes, par exemple, la présence de nombreuses personnes extérieures non autorisées. L'isolement des locaux ne s'avère efficace que si l'équipe est

suffisamment importante pour que le prestataire lui dédie un étage entier, naturellement isolé du reste des locaux.

> **EN RÉSUMÉ**
> **Isolement des équipes**
> L'isolement des équipes en offshore devrait toujours être réalisé lorsque ces dernières sont importantes et qu'on recherche un niveau de sécurité ou de confidentialité élevé. En isolant les équipes et le matériel et en les dédiant à l'activité du client, on parvient à se démarquer des règles en vigueur chez le prestataire et à appliquer les procédures qui conviennent le mieux.

Les fuites chez des concurrents

Les clients peuvent craindre que le prestataire fournisse des prestations à un concurrent et qu'une partie du savoir ou que certaines informations confidentielles soient divulguées à cette occasion. Ce risque est particulièrement important pour les éditeurs de logiciels.

La nature des informations confidentielles peut concerner les spécifications, des parties du code source, des informations sur le plan produit, etc. Un collaborateur passant d'un client à un autre ou, pire, une personne travaillant à temps partiel sur deux projets différents du prestataire peut transmettre de telles informations à la concurrence, sans toujours s'apercevoir de leur valeur.

Certains contrats essaient de se prémunir contre de tels risques. Une autre solution consiste bien sûr à créer une filiale ou un joint-venture en offshore afin de contrôler pleinement les activités de la société. Il est aussi possible d'identifier les autres clients du prestataire et d'interdire éventuellement à ce dernier de travailler avec certains d'entre eux (*voir le chapitre* 9).

> **EN RÉSUMÉ**
> **Se protéger des fuites vers les concurrents**
> Un client qui redoute que le prestataire offshore traite avec un concurrent et que des informations confidentielles lui parviennent peut se protéger par contrat. Il est de la sorte possible d'interdire au prestataire de traiter avec des concurrents figurant nommément dans le contrat. Cette interdiction perdure souvent après la fin du contrat.

Réutilisation du code source

Dans les pays où la propriété intellectuelle est une notion pour le moins vague, on peut craindre que certains candidats à un emploi chez un prestataire ne cherchent à faire valoir non seulement leurs capacités propres, mais aussi le code source et autres éléments qu'ils ont emportés d'un emploi précédent. Malheureusement, certaines sociétés ne rejettent pas systématiquement de telles propositions et se laissent tenter.

Dans de nombreux pays, les programmeurs quittent la société qui les employait en emportant leur code source, voire le code source complet du projet sur lequel ils travaillaient. Ils n'ont pas nécessairement l'intention de le réutiliser, mais ils le conservent en souvenir de leur travail. Certains d'entre eux vont parfois plus loin et réutilisent sans le dire dans de nouveaux projets des portions de code déjà produites pour peu que les technologies employées le permettent. Inutile de préciser que ces pratiques ne sont pas spécifiques de l'offshore et qu'on les constate aussi dans nos pays, où elles sont tout aussi difficiles à contrôler.

Si l'on ne peut totalement s'en prémunir, du moins peut-on les rendre plus difficiles à réaliser. Tout d'abord, on s'assure que tous les employés signent l'accord de confidentialité précisant quelles sont les informations confidentielles, ainsi que les règles les concernant et les risques encourus par l'employé qui ne les respecteraient pas. La gestion du référentiel permet ensuite de savoir si une personne a tenté de retirer l'ensemble du contenu du projet sans raison.

EN RÉSUMÉ

Protection contre la réutilisation de code

On peut partiellement se protéger contre la réutilisation de son code source en demandant à chaque collaborateur de signer un accord de confidentialité qui engage sa responsabilité personnelle en cas réutilisation de ce code dans d'autres réalisations.

Protection de la méthode

Certains clients, notamment les sociétés de services, considèrent que leurs méthodes, procédures et documents de suivi font partie intégrante de leur valeur, voire leur donnent un avantage concurrentiel. Il est essentiel pour eux que la valeur attribuée à la méthode soit perçue comme telle par le prestataire.

Ces éléments sont particulièrement vulnérables en offshore. La confi dentialité des méthodes est rarement comprise, et la plupart des informaticiens n'hésitent pas à les réutiliser voire à les communiquer à des tiers. Ils le font le plus souvent sans malice et s'imaginent simplement qu'ils en ont le droit. Il n'est pas facile de se protéger de ce risque de fuite, surtout si la méthode synthétise des bonnes pratiques qui n'ont par ailleurs rien d'innovant .

La meilleure solution est d'insérer ce sujet dans les formations réalisées sur place et d'ajouter les méthodes aux informations confidentielles clairement identifiées dans l'accord de confidentialité.

Augmentation brutale des coûts des prestations

Un prestataire offshore peut souhaiter augmenter le tarif de ses prestations, par exemple lorsque les salaires des informaticiens connaissent une hausse brutale dans le pays. De telles situations résultent généralement de l'âpre concurrence que se livrent les prestataires ou d'une demande accrue liée à l'implantation de grandes sociétés étrangères. Il se peut aussi que l'inflation en dollars engendre une forte réduction du pouvoir d'achat. Le prestataire souhaite en ce cas ajuster ses tarifs pour retrouver la valeur de sa facturation en début de contrat. Certains contrats prévoient d'ailleurs d'indexer les prestations sur le taux d'inflation en dollars ou en euros.

Quelles qu'en soient les raisons, il arrive que le prestataire exprime le besoin d'augmenter fortement ses tarifs.

EN RÉSUMÉ

Ajustement des prix sur l'économie du pays

Il est commun de prévoir un ajustement des tarifs du prestataire en fonction du taux d'inflation en dollars ou en euros. Faute de cela, le prestataire risque de ne plus retrouver sa marge dans les prestations fournies.

Il n'est pas rare que le prestataire demande une réévaluation de ses tarifs parce qu'il a fait une proposition initiale trop basse afin d'obtenir le contrat. Il attend généralement un an avant de demander un tel ajustement et masque les véritables raisons du problème derrière des considérations économiques on conjoncturelles.

Les différences de tarifs entre un nouveau contrat et les précédents chez un même prestataire peuvent aller du simple au double, voire davantage si la comparaison porte sur des prestations au forfait et en régie. Certains projets calculés au plus juste au commencement du contrat ne génèrent plus aucune marge. Le risque est alors que le prestataire se désintéresse des projets à faible marge et en retire les meilleurs de ses collaborateurs pour les affecter à des projets plus profitables.

Le client ne doit donc pas s'enorgueillir des bas tarifs qu'il a négociés en offshore par rapport à ceux pratiqués par son prestataire avec d'autres clients car il n'en aura que pour son argent. Pour accepter ces tarifs, le prestataire a dû recruter les candidats qui acceptaient les salaires les plus bas, les meilleurs profils et les plus stables ayant échu aux autres clients.

> **EN RÉSUMÉ**
> **Bas tarifs et qualité des prestations**
> Il n'est pas souhaitable que les tarifs pratiqués pour un client soient largement inférieurs à ceux appliqués aux autres clients du prestataire. L'équipe du client sera vite identifiée comme étant à faible marge et sera négligée, voire utilisée pour construire d'autres équipes pour d'autres clients. Le personnel sera clairement de qualité inférieure, ce qui se ressentira sur la productivité et la qualité des prestations.

Il est généralement suffisant de se situer dans une moyenne raisonnable des tarifs appliqués chez le prestataire, sans nécessairement s'aligner sur les plus élevés.

En cas de tarifs exagérément bas, le prestataire ne manque pas d'émettre des requêtes afin de les ajuster. Le client aurait tort d'ignorer systématiquement ces requêtes, car certaines demandes d'ajustement peuvent être justifiées. C'est le cas, par exemple, lorsque le client a négocié des conditions spéciales pour couvrir une période financièrement difficile pour lui et que ces conditions perdurent alors que sa situation s'est améliorée.

Si le prestataire ne parvient pas à se faire entendre, il peut frapper un grand coup sur la table et exiger l'ajustement, en menaçant de ne pas livrer les codes source et autres livrables, voire de dissoudre l'équipe. Le client porte alors sa part de responsabilité dans la crise. En ignorant les demandes du prestataire, il s'est exposé au risque de voir ce dernier préférer arrêter un partenariat qui ne lui apporte pas de marge. Il ne s'agit pas là vraiment d'un chantage.

Monter deux équipes en offshore

Pour se prémunir de tout risque en offshore, il est envisageable de monter deux équipes chez des prestataires différents, chaque équipe appliquant strictement les mêmes procédures et méthodes. En cas de problème avec l'un des prestataires, on bascule les tâches sur l'autre, et ce, d'autant plus facilement que les règles de codage, de documentation et de reporting sont les mêmes sur les deux sites.

Cette solution doit être notamment considérée pour tout projet un tant soit peu stratégique. Elle implique cependant un coût plus important. La gestion des projets répartis est beaucoup plus délicate, les problèmes de communication, de synchronisation et surtout

d'intégration multisite faisant perdre en productivité et induisant un coût plus important. Les visites sur place sont également plus longues et coûteuses, car au lieu de rendre visite à une seule équipe, on se déplace sur les deux sites.

Le montage de deux équipes peut être considéré de plusieurs façons. Il est possible de monter deux équipes de taille comparable, qui collaborent au même projet. Les réalisations sont distribuées sur les équipes de façon à confier à chacune un ensemble fonctionnel aux dépendances externes faibles. Chaque équipe peut donc travailler indépendamment de l'autre. Le résultat du travail des deux équipes est ensuite assemblé pour construire le produit final. On atteint de la sorte plusieurs objectifs : on s'assure une solution de repli si l'un des prestataires venait à se révéler défaillant, et aucun des deux sites ne dispose de la totalité du produit, ce qui est un gage de sécurité. En revanche, les projets doivent être synchronisés entre les équipes, et les points de dépendance des réalisations doivent être gérés avec précision.

Cette organisation ne manque pas de créer une concurrence entre les équipes, qui, bien gérée, peut se traduire par une augmentation de la productivité de chaque équipe. Elle peut à l'inverse devenir néfaste si chacune des équipes cherche à établir sa prééminence, par exemple, en ne fournissant pas de réponses aux questions posées par l'autre équipe ou en traînant pour livrer les éléments qui lui sont nécessaires.

On peut aussi choisir de créer une équipe principale et une équipe de repli, beaucoup plus petite. L'essentiel des réalisations est donné à l'équipe principale, la seconde se voyant confier de petites réalisations indépendantes ou peu importantes. Il importe en ce cas de s'assurer que la petite équipe connaît le produit et les méthodes en vigueur. En cas de nécessité, la petite équipe servira de noyau à une équipe rapidement construite.

Les surcoûts opérationnels sont dans ce cas assez faibles car le client se concentre sur l'équipe principale et ne perd pas de temps à gérer l'équipe secondaire.

On peut encore considérer de confier à deux équipes en parallèle les mêmes réalisations. Les coûts sont alors doublés. Cette approche ne manque pas de créer une vive concurrence, car les réalisations des deux équipes sont directement comparables, et le travail de la meilleure équipe part en production, sanctionnant ainsi l'équipe perdante. Une épée de Damoclès pend sur l'équipe la moins performante, qui risque à tout moment de se voir dissoute sans que cela affecte le moins du monde les réalisations du client. Le gain en productivité peut, dans une certaine mesure, compenser le doublement des coûts.

Le tableau 6.1 résume les avantages et inconvénients de chaque approche.

Tableau 6.1. Avantages et inconvénients de la création de plusieurs équipes en offshore

	Deux équipes de même taille se partageant le projet	Une équipe principale et une petite équipe de repli	Deux équipes effectuant les mêmes réalisations
Productivité	L'impact sur la productivité peut être positif s'il existe une saine émulation ou négatif si l'une tente de nuire à l'autre pour établir sa prééminence.	Similaire à une équipe unique	Concurrence très forte en permanence et compétitivité accrue

Tableau 6.1. Avantages et inconvénients de la création de plusieurs équipes en offshore*(suite)*

	Deux équipes de même taille se partageant le projet	Une équipe principale et une petite équipe de repli	Deux équipes effectuant les mêmes réalisations
Confidentialité	Les réalisations sont partagées entre les équipes qui ne voient, chacune, qu'une partie du produit complet.	L'équipe principale dispose de tout le produit. L'équipe de repli peut ne disposer que d'une vue partielle.	La confidentialité est réduite, car les deux équipes disposent du produit complet.
Protection contre un problème avec le partenaire	Repli aisé de toutes les réalisations sur un site unique. La bonne application des méthodes rend ce transfert beaucoup plus facile.	Le repli sur la petite équipe est assez délicat, car de nombreux postes doivent être rapidement pourvus et le matériel est souvent sous-dimensionné.	Le passage d'une équipe à une autre se fait sans heurts.
Impact sur les coûts	Les surcoûts sont surtout organisationnels (déplacements et matériels).	Faibles surcoûts si l'on restreint les déplacements et les investissements chez le prestataire de repli.	Les coûts sont doublés pour les prestations offshore. Les déplacements sont également doublés.

Les paiements du client

Nous avons déjà abordé certains effets de l'absence ou du retard de paiement des factures du prestataire par le client. Les réactions du prestataire sont, dans l'ordre, de bloquer les livrables, de menacer de dissoudre l'équipe, de dissoudre effectivement l'équipe et disposer du produit à sa convenance. Il est rare qu'il décide de poursuivre son client, sauf dans le cas où il aurait une représentation dans le pays de ce dernier.

Lorsqu'un conflit réel surgit entre le prestataire et le client, celui-ci peut décider de ne pas payer son prestataire. Le conflit peut avoir pour origine des clauses contractuelles non respectées, une productivité anormalement basse ou encore un taux de démission ou de licenciement révélant un problème de management local. Il vaut alors mieux payer le prestataire partiellement de façon à exercer une pression forte mais raisonnable pour le contraindre à honorer ses engagements.

Les retards de paiement

Comme expliqué au chapitre 3, le fait de payer en retard résulte le plus souvent en un retard de paiement de l'équipe offshore. La régularité des paiements est donc un des facteurs les plus appréciés des prestataires comme des collaborateurs. Un client qui fait de son mieux pour régler au plus tôt le prestataire est d'autant mieux valorisé et donc servi. De plus, la régularité des paiements peut venir compenser en grande partie une marge faible et faire en sorte que le client ne soit pas négligé.

Payer dans les temps n'est pas toujours chose facile. Si les éléments pour établir la facture sont un tant soit peu complexes — bien souvent, elles prennent en compte le nombre de jours travaillés par collaborateur, mais aussi les vacances, les heures supplémentaires et des éléments refacturés à prix coûtant —, le prestataire peut facilement commettre des erreurs de facturation. Certaines erreurs sont difficiles à détecter. Par exemple, il se peut que l'on ait défini par contrat un nombre de jours de congé annuel minimal pour les collaborateurs et qu'aucun d'eux ne puisse être facturé sur l'année pour plus de jours que le maximum défini. Pour vérifier la facture, le client doit pointer pour chaque collaborateur le nombre de jours de congés qu'il a effectivement pris afin de vérifier qu'il n'est pas facturé au-delà de ce qui est prévu ou encore vérifier qu'un jour férié en offshore n'apparaît pas comme un jour travaillé.

Les corrections de factures peuvent générer de nouvelles erreurs. Le temps s'écoule alors sans engager de paiement. Si un décideur est en vacances, en voyage ou simplement peu disponible, les allers-retours prennent parfois des semaines, pendant lesquelles les collaborateurs mécontents ne sont pas payés.

Il est possible de s'entendre pour que les factures soient honorées à réception, quitte à ce que les ajustements éventuels soient reportés sur la facture suivante.

Les risques politiques locaux

Comme expliqué au chapitre 2, les pays de l'offshore peuvent présenter des risques d'instabilité politique ou économique. À moins d'événements d'une réelle gravité, la vie économique est peu affectée, et les informaticiens continuent de travailler, parfois au prix d'une perte de productivité ou d'un absentéisme accru.

Seules les crises de grande ampleur peuvent arrêter un projet. Il ne s'agit pas alors d'événements isolés mais de catastrophes naturelles, de guerres civiles ou d'autres séismes majeurs. Les événements politiques qui ont marqué la fin du régime de Ceausescu en Roumanie ont à peine perturbé les prestations des équipes roumaines en offshore. Il en est allé de même en Ukraine, où les manifestations massives de contestation de l'élection présidentielle de 2004 n'ont en rien perturbé les projets offshore en cours.

Dans certains pays, les risques en matière de sécurité sont tels que les chefs de projet des sociétés clientes refusent de se rendre sur place. Cela concerne de très nombreux pays, et même l'Inde, le premier pays de l'offshore, a plusieurs fois frôlé la guerre avec le Pakistan.

Le choix d'un pays de l'offshore doit tenir le plus grand compte de ce type de risque, même s'il n'a pas de lien direct avec le coût des prestations. Le premier effet des situations à risques est le refus des chefs de projet locaux et autres collaborateurs de se rendre chez le prestataire.

Les licences des outils de développement

Le risque juridique que fait peser l'emploi par le prestataire de logiciels sans licence est difficile à évaluer. Dans la plupart des pays de l'offshore, en effet, les droits d'utilisation

des logiciels sont pour le moins équivoques, et l'on trouve des éditions complètes de Windows XP, Oracle Server ou Microsoft Exchange Server, par exemple, pour quelques dollars. Il ne s'agit pas pour autant de versions pirates, puisqu'elles comportent les timbres ou hologrammes attestant que des droits ont été versés au gouvernement sur la vente de ces marchandises.

La crainte d'être poursuivi pour avoir bénéficié de licences illégales est loin d'être infondée. On peut s'en protéger en exigeant par contrat que les logiciels mis à la disposition du client soient acquis en pleine conformité avec les lois du pays. Le prestataire, et non le client, est tenu de s'assurer que cette clause est respectée. On peut aussi demander confirmation écrite que tous les produits ont été acquis officiellement.

Le problème se complique lorsque c'est la légalité même des licences qui laisse à désirer. Nombre de gouvernements des pays de l'offshore permettent que des logiciels sans licences soient vendus en toute légalité dans des magasins officiels et en perçoivent les taxes afférentes. Chacun a beau savoir que les droits de ces logiciels ne sont pas acquittés à l'éditeur, cela reste le moyen d'acquisition de logiciels le plus naturel dans ces pays.

Même avec la meilleure volonté, il est bien difficile de vérifier que les licences que le prestataire utilise ont été acquises en toute légalité. Certaines licences en apparence légales peuvent avoir été upgradées illégalement ou déployées sur plus de machines qu'autorisé, par exemple.

Lorsque le réseau est géré par le prestataire offshore, le client peut se satisfaire d'une simple vérification que les licences sont légalement acquises. Il n'en va pas de même si le réseau est dédié à un client, dans une filiale ou dans un joint-venture, par exemple. Le client peut être tenu pour responsable de la gestion des licences sur son réseau, puisqu'elles ont été déployées selon ses directives. Il est en ce cas nécessaire qu'il s'assure de la légalité de toutes les licences.

Il est cependant peu probable qu'une organisation quelconque dans un pays de l'offshore ait les moyens de contraindre un prestataire à se soumettre à un audit pour vérifier la légalité des licences déployées.

> **EN RÉSUMÉ**
> **Vérification des licences en offshore**
>
> Lorsque le réseau est géré par le prestataire, il doit être établi contractuellement que ce dernier met à disposition du client des licences logicielles acquises légalement selon les lois du pays. Lorsque le client gère son propre réseau dédié, c'est à lui de faire la preuve qu'il a acquis les licences des logiciels qu'il utilise.

Les licences apportées par le client

Une difficulté symétrique concerne les licences des logiciels apportés par le client afin d'être utilisés en offshore. Dans ces pays, le marché parallèle des logiciels — qui est en fait le marché principal — est à l'affût de toutes les nouvelles versions des produits. Il y a donc un risque que la version apportée par le client devienne la souche de duplications illicites.

Pour les logiciels de très grande diffusion, comme les systèmes d'exploitation, les suites bureautiques, la CAO ou l'édition de vidéos, les pirates trouvent très facilement les sources qui leur permettent de sortir les versions récentes sur les marchés parallèles en même temps voire avant leur sortie officielle. En revanche, certains logiciels professionnels

coûteux ne sont pas toujours disponibles rapidement sur ces marchés. Lorsqu'un client de l'offshore arrive avec un produit réputé rare, il se peut que celui-ci soit immédiatement copié pour être revendu à des structures qui se chargent de le dupliquer. Les moyens de lutte contre les experts du piratage que l'on trouve dans ces pays étant généralement inopérants, une fois la copie du logiciel transmise, elle échappe à tout contrôle.

L'éditeur du logiciel peut se retourner contre le client, lequel est censé faire des efforts raisonnables pour protéger les licences mises à sa disposition, d'autant plus si le produit dupliqué a conservé le numéro de série attribué à la version du client.

Pour se protéger de ce type de fraude, la meilleure solution reste d'alerter le prestataire. Les accords de confidentialité peuvent inclure les produits logiciels originaux et exiger que le prestataire et les collaborateurs les protègent d'une diffusion frauduleuse.

Retrait des protections des logiciels

Lorsqu'on apporte un produit logiciel en offshore, on est fréquemment surpris d'entendre les administrateurs réseau demander s'ils peuvent en déployer une version sans protection, beaucoup plus facile à gérer, quand ils ne le font pas de leur propre chef, sans même poser la question. Le paradoxe est que les limitations des verrouillages pénalisent ceux qui ont acquitté les licences alors que ceux qui utilisent ces mêmes produits piratés les déploient et les réinstallent comme ils le souhaitent.

Les textes qui accompagnent les licences précisent souvent que l'on ne doit pas essayer de retirer les systèmes de protection. On a beau informer les services informatiques internes du prestataire qu'ils doivent déployer les licences conformément aux directives de l'éditeur, on constate bien souvent dans la réalité que les produits ont été déployés sans protection. Il suffit pour s'en convaincre de demander un redéploiement et de constater que celui-ci ne fait l'objet d'aucune question posée à l'éditeur, alors même que les méthodes de verrouillage employées sur ces logiciels demandent d'entrer des numéros fournis par le support client à chaque opération majeure.

Les risques sociaux chez le client

Les risques sociaux en local, chez le client, ont été brièvement introduits au chapitre 3 pour souligner l'importance de la communication de la société locale pour expliquer à ses équipes sa stratégie en offshore. Cette communication vise à réduire les forts risques d'incompréhension des objectifs des réalisations en offshore, surtout si la société n'a pas l'intention de se séparer de ces équipes pour les délocaliser. En l'absence de communication, les collaborateurs locaux supposeront que la société a les pires intentions.

Les syndicats et les représentants du personnel manquent rarement de s'opposer à l'utilisation de ressources en offshore, dans laquelle ils ne voient que la menace que les employés de la société soient délogés au profit de personnels distants engagés à vil prix.

On aura beau expliquer que cette décision apportera plus de force à la société, qui pourra mieux se placer face à ses concurrents, que l'intérêt des employés locaux pour leur travail s'en trouvera renforcé en leur permettant de se concentrer sur les tâches les plus créatives ou que cet apport à la capacité de production nécessitera davantage de ressources locales

et résultera probablement en embauches, on n'évitera pas complètement les risques de rejet par les équipes locales.

Une bonne communication interne peut réduire considérablement ces risques, surtout si elle est poursuivie dans le temps et non ponctuelle. Si la société fait la preuve que ses actions sont en phase avec son message, les inquiétudes tombent assez rapidement. Il importe surtout de communiquer sur les affaires remportées grâce à l'offshore en démontrant qu'elles n'auraient pu l'être autrement.

> **EN RÉSUMÉ**
> **Inquiétudes du personnel local**
> Lorsqu'une société commence à travailler avec un prestataire en offshore, sa communication locale est indispensable pour réduire les inquiétudes du personnel. Une communication réussie met en avant les avantages que l'entreprise et ses employés en retireront.

Un changement de méthodologie et d'organisation du développement visant à intégrer une démarche industrielle peut susciter le malaise chez certains membres des équipes de développement. Comme expliqué précédemment, ce sont les profils polyvalents qui sont les plus inquiets, car une telle réorganisation réduit le plus souvent leur poste, auparavant transversal, à une fonction. L'expérience prouve toutefois que ces personnes démissionnent rarement, surtout si le management prend soin de leur confier des missions valorisantes.

D'une façon générale, le passage à l'offshore s'effectue plutôt bien, après une période de crise inévitable mais rarement longue.

Conclusion

La meilleure façon de limiter les risques de toute nature avec un prestataire en offshore est de parvenir à créer une communauté d'intérêts avec lui. Si la réussite du client doit être également celle du prestataire, les problèmes se règlent d'eux-mêmes. À l'inverse, lorsque le client perd confiance, négocie tous les prix, essaie de réduire en permanence la marge du prestataire ou investit en audits pour vérifier que les directives sont appliquées, la relation de partenariat se détériore immanquablement. La contrainte devenant externe au prestataire, celui-ci porte moins d'attention à protéger les intérêts de son client.

Lorsque le prestataire réalise que son partenariat est solide et fiable, il souhaite s'y investir à long terme, et les opérations se déroulent mieux. Les audits deviennent dès lors pratiquement inutiles, le prestataire défendant les intérêts du client en même temps que les siens.

PARTIE 2

Préparation des projets en offshore

La première partie de l'ouvrage a introduit la culture de l'offshore et décrit le fonctionnement et les motivations des prestataires qu'on y rencontre. La présente partie aborde la préparation des projets en offshore, qui commence par le choix du projet à confier au prestataire. En association avec ce projet, le client doit aussi choisir un mode de fonctionnement convenant à la fois à ses préférences et à la nature du projet à réaliser.

Une fois choisi le projet à réaliser en offshore, vient la question essentielle du choix du prestataire, qui découle pour l'essentiel des préférences du client et du type de projet à réaliser. C'est un choix déterminant, car selon la localisation, et donc la culture, du prestataire, certains modes de fonctionnement sont permis tandis que d'autres sont interdits.

La mise au point du contrat qui lie le client et le prestataire constitue la dernière étape de cette phase préparatoire. C'est une étape cruciale, qui doit permettre de définir les détails de la coopération avec le prestataire concernant tout à la fois le fonctionnement quotidien, les éléments facturables, la gestion des relations humaines et les limites de responsabilité des deux parties.

Référence de la relation, le contrat donne en outre le ton de la coopération. Trop dur, il met le prestataire sur la défensive et rate son objectif, qui est de réunir les conditions du succès. Trop permissif, il donne lieu à des dérives, que l'on ne parvient plus à contrôler. Le bon équilibre est difficile à atteindre, et l'on ne peut y parvenir que par une gestion précise de tous les éléments qui le constituent.

Cette partie s'achève sur les grands principes qui président à la gestion de projet en offshore.