RISQUE OPÉRATIONNEL
Gestion juridique des risques liés aux nouvelles technologies

Franklin Brousse

Avocat
Cabinet Bird & Bird
franklin.brousse@twobirds.com

L'accord de Bâle II traite explicitement du risque opérationnel. Celui-ci intègre les nombreux aspects juridiques et pénaux liés aux systèmes d'information et aux nouvelles technologies.

L'accord de Bâle II sur le contrôle bancaire du 26 juin 2004 traite pour la première fois explicitement du risque opérationnel, c'est-à-dire notamment l'erreur humaine, le dysfonctionnement des systèmes ou la fraude. Mais il comprend aussi les aspects juridiques, particulièrement lorsqu'ils concernent les systèmes d'information. En effet, la gestion des risques opérationnels passe par une intégration des aspects juridiques et pénaux, nombreux en matière de nouvelles technologies, quelle que soit l'approche de gestion des risques opérationnels retenue par la banque ("indicateur de base", "standard", "mesures avancées"). En outre, l'accord de Bâle II impose une obligation de *reporting* sur les risques opérationnels concernant tous les domaines de l'activité. Celui-ci doit intégrer une dimension juridique, s'agissant de l'exploitation de systèmes d'information fermés mais aussi de plus en plus ouverts au public et à la clientèle.

LA GESTION DES RISQUES DE FRAUDE

La sécurité et les conditions d'exploitation des systèmes d'information figurent parmi les problématiques à intégrer dans la gestion des risques opérationnels. Outre les fraudes externes, les banques font face à la montée en puissance des menaces internes, souvent sous-estimées selon de récentes études. Il s'agit tout d'abord d'identifier le rôle et les responsabilités de tous les acteurs de l'entreprise concernés par la sécurité informatique, de la direction des systèmes d'information aux intervenants extérieurs, en passant par les salariés qui représentent aujourd'hui le premier facteur de risque, ces derniers étant souvent à l'origine de vols, de pannes, d'erreurs d'utilisation ou de malveillances. Ce préalable permet de mener en interne une politique de dissuasion fondée sur des règles de sécurité clairement définies et opposables (par le biais d'une charte de sécurité, de notes internes, ou par la modification du règlement intérieur) ainsi que sur la sensibilisation, l'information et la formation des salariés. Les risques liés aux interventions de prestataires sur les systèmes d'information doivent être traités de façon spécifique par les dispositions contractuelles régissant les conditions de leurs interventions, notamment lorsqu'elles sont réalisées à distance, dans le cadre de services de télémaintenance, ou lorsqu'elles touchent directement ou indirectement à des données de l'entreprise par définition sensibles et confidentielles.

Dans cette situation, l'élaboration d'un plan de gestion des atteintes aux systèmes d'information sera utile pour définir les actions techniques et juridiques à mettre en œuvre en cas d'atteintes.

UN PLAN DE GESTION DES ATTEINTES AUX SYSTÈMES

L'établissement de ce plan permet aux banques de se donner les moyens de réagir rapidement et efficacement contre toute atteinte, quelles qu'en soient la nature et l'origine, et d'exercer un recours judiciaire efficace. À ce titre, les banques ne peuvent exercer de recours efficace si elles n'ont pris aucune mesure préventive, notamment en termes d'administration des preuves et des traces infor-

matiques qui conditionnent, en grande partie, la pertinence et l'efficacité de ces recours.
Les banques utilisant de plus en plus le nouveau canal de distribution que constitue l'internet, s'exposent à des risques inédits liés à de nouvelles pratiques commerciales intervenant dans un cadre juridique particulièrement protecteur envers les consommateurs. En effet, la loi du 21 juin 2004 pour la Confiance dans l'économie numérique dite "LCEN" délimite strictement la "relation client" dans le cadre de services en ligne.
Le non-respect de ces nouvelles dispositions peut entraîner des sanctions pénales et tombe également sous le contrôle de la Commission nationale informatique et libertés (CNIL) dont les pouvoirs de sanction financière viennent d'être récemment renforcés avec l'adoption de la loi du 6 août 2004 modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

« Les banques ne peuvent exercer de recours efficace si elles n'ont pris aucune mesure préventive, notamment en termes d'administration des preuves et des traces informatiques. »

L'UTILISATION DES DONNÉES À CARACTÈRE PERSONNEL

La réforme de la loi du 6 janvier 1978 a modifié sensiblement les obligations des entreprises en matière de gestion des données nominatives, en introduisant notamment la faculté de désigner un correspondant à la protection des données à caractère personnel, afin de bénéficier d'un allègement de ses obligations déclaratives. La désignation d'une telle personne devrait s'inscrire naturellement dans le cadre d'une gestion des risques opérationnels liés aux données nominatives relatives

DÉFINITION

Le risque opérationnel est défini comme le risque de pertes résultant de carences ou de défauts attribuables à des procédures internes, au personnel et aux systèmes ou à des événements extérieurs.

RÉGLEMENTATION

La relation client dans le cadre des services en ligne

■ La prospection directe par télécopieur ou courrier électronique sans consentement préalable de la personne est désormais interdite. La notion de prospection directe est large puisqu'elle vise notamment l'envoi de tout message destiné à promouvoir, directement ou indirectement, des services ou l'image d'une personne fournissant des services. La seule exception au principe du consentement préalable réside dans la prospection directe par courrier électronique des personnes ayant déjà bénéficié de services, mais uniquement pour des services analogues fournis par la même personne morale, ce qui limite considérablement le champ de prospection auprès des clients.

aux salariés et aux clients exploitées par les banques. Bien évidemment, les banques seront tentées de se prévaloir des obligations nées de l'accord de Bâle II pour augmenter le nombre de données collectées auprès de leurs clients et prospects. La gestion des risques opérationnels ne doit toutefois pas conduire à des collectes de données non pertinentes ou excessives au regard de la finalité des traitements qui seront réalisés sous le contrôle de la CNIL. Il s'agit de respecter, en toute hypothèse, les droits des clients et prospects sur les données les concernant, cette gestion des risques ne pouvant servir de quelconque justification, particulièrement aux yeux de la CNIL. Le système de gestion des risques opérationnels conduit, le plus souvent, à la mise en œuvre d'outils de traçabilité et de surveillance permettant un contrôle de l'activité des salariés.

LA CONFORMITÉ AU REGARD DU DROIT DU TRAVAIL

Les banques devront évaluer l'opportunité de saisir les instances représentatives du personnel, conformément aux dispositions du Code du travail. Il s'agira de procéder à un contrôle a priori de la conformité des processus de gestion et des systèmes de mesure des risques au regard de la réglementation applicable en matière de droit du travail, en lien avec celle applicable en matière de protection des données à caractère personnel relatives aux salariés. Ce contrôle devra être intégré dans l'étape de validation du système de mesure des risques, tout comme l'ensemble des aspects juridiques liés à la gestion des risques opérationnels.

ÉVALUATION CONTRACTUELLE DES RISQUES LIÉS AUX SYSTÈMES D'INFORMATION

Par ailleurs, les banques devront mener un audit des contrats existants relatifs à leurs systèmes d'information mais nécessitant des modifications liées à la mise en œuvre de leur système de mesure des risques. En fonction des dispositions contractuelles applicables, les banques pourront envisager une négociation de la répartition des coûts liés à la mise en conformité de tout ou partie de leur système d'information. En effet, certains contrats contiennent des clauses de conformité à la loi en application desquelles le prestataire informatique s'engage à garantir que son produit ou son service reste conforme aux lois et réglementations en vigueur pendant la durée du contrat. De telles clauses ont des répercussions juridiques importantes, parce qu'elles signifient que techniquement, le prestataire aura à sa charge tout ou partie des coûts induits par les changements de lois et de réglementations, comme dans le cas de l'accord de Bâle II, qui devrait entrer prochainement dans notre champ législatif par le biais d'une directive le transposant dans la réglementation européenne puis française.

« Certains contrats contiennent des clauses de conformité à la loi en application desquelles le prestataire informatique s'engage à garantir que son produit ou son service reste conforme aux lois et réglementations en vigueur pendant la durée du contrat. »

GESTION DU RISQUE PÉNAL

Enfin, il convient de souligner qu'en matière de nouvelles technologies et de systèmes d'information, le risque opérationnel est souvent associé à un risque pénal, les infractions étant de plus en plus nombreuses en ces domaines. Ainsi, le risque pénal est présent dans chacune des catégories de risques opérationnels susvisées (fraudes, pratiques commerciales, protection des données personnelles, contrôle d'activité, etc.). Une cartographie de ce risque devra donc être établie dans le cadre de la gestion des risques opérationnels, et intégrée au sein du système de mesure des risques.

De nombreuses banques et institutions financières ont déjà pris du retard dans leurs préparatifs concernant le risque opérationnel, car elles doivent faire face à de nombreux obstacles afin de réussir ce nouveau challenge réglementaire. Il ne faudrait pas pour autant négliger les aspects juridiques liés aux risques opérationnels, particulièrement lorsqu'ils concernent les systèmes d'information, car les enjeux restent significatifs. ■