SÉCURITÉ DES SYSTÈMES INFORMATIQUES
Règles applicables et limitation des responsabilités*

Antoine Juaristi
Avocat à la Cour
Lovells

Daphné Renault
Avocat à Cour
Lovells

La décision rendue le 15 juillet 2009 par la Commission bancaire** conduit à rappeler la teneur des obligations qui pèsent sur les établissements de crédit s'agissant de leurs systèmes d'informations et à s'interroger de façon légitime sur l'étendue de leur responsabilité.

La Commission bancaire a récemment rendu une décision de sanction prenant la forme d'un blâme et d'une amende d'un montant de 20 millions d'euros [1], en raison du non-respect de dispositions relatives au contrôle interne dans le domaine des opérations de marché, qui sont qualifiées d'essentielles par la Commission bancaire. À l'instar de sa décision du 8 juillet 2008, la Commission ban-

[1] **Cette décision constitue la première application de l'article 159 de la loi de modernisation de l'économie du 4 août 2008, ayant multiplié par 10 le montant maximum des sanctions financières pouvant être prises par la Commission bancaire, lequel est donc désormais de 10 fois le montant du capital minimum auquel est astreinte la personne morale sanctionnée.**

* Avec la contribution de Rachel Tort, juriste

** Bulletin officiel du CECEI et de la Commission bancaire de juillet 2009, n° 17, p. 4.

caire relève, dans celle de juillet 2009, des infractions incluant la violation de la réglementation applicable à la sécurité des systèmes d'information (SI). Force est de constater que la réglementation relative à la sécurité des systèmes informatiques des établissements de crédit et des prestataires de service d'investissement n'a pas évolué de manière radicale ces dernières années.

Néanmoins, un certain nombre d'affaires retentissantes a récemment mis en cause la sécurité des systèmes informatiques des établissements bancaires, au premier rang desquelles l'affaire Kerviel, laquelle est revenue sur le devant de la scène avec la demande du procureur de la République visant le renvoi de ce dernier devant le tribunal correctionnel. On peut par ailleurs constater que les cours et tribunaux ont rendu quelques décisions remarquées en matière de transactions boursières par voie électronique.

Il est dès lors opportun de faire un point sur cette matière aux textes abondants et d'origine variée, tant au plan national qu'au plan communautaire, et d'apporter un éclairage sur les responsabilités pouvant découler pour les établissements de crédit, tant d'un manquement à leurs obligations réglementaires relatives à la sécurité de leurs SI, que d'une défaillance de ces systèmes, et ce vis-à-vis de leur autorité de tutelle et de leurs clients.

PANORAMA DES OBLIGATIONS RÉGLEMENTAIRES DES ÉTABLISSEMENTS DE CRÉDIT

Sous l'influence des autorités de tutelle, mais aussi de divers groupes de travail nationaux et internationaux [2], les préconisations en matière de sécurité des SI ont été nombreuses. Aujourd'hui, il est nécessaire de garder à l'esprit que la sécurité informatique fait partie intégrante du dispositif prudentiel des établissements de crédit. En ce sens, elle doit être comprise comme une composante même des questions de gestion des risques et, par voie de conséquence, une composante du contrôle interne, dont les insuffisances sont immanquablement et sévèrement sanctionnées (*voir l'encadré 1*).

En droit interne, les obligations en matière de sécurité informatique pesant sur les établissements de crédit et les entreprises d'investissement, autres que les sociétés de gestion de portefeuille, sont essentiellement définies par le règlement n° 97-02 du Comité de la réglementation bancaire et financière (CRBF) modifié, relatif au contrôle interne des établissements de crédit et des entreprises d'investissement.

Les prestataires de services d'investissement (PSI) se voient, quant à eux, appliquer les dispositions de l'Ordonnance n° 2007-544 du 12 avril 2007 relative aux marchés d'instruments financiers, ainsi que les dispositions spécifiques du Code monétaire et financier [3].

En pratique, l'ensemble des principes qui découlent de ces textes sont le résultat de la transposition de directives européennes et les obligations qui en résultent pour les établissements de crédit et les PSI sont très comparables, pour ne pas dire identiques. Les établissements de crédit demeurent libres de « *déterminer le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers* » [4]. En revanche, ils ont pour obligation de mettre en place un contrôle de leurs SI de manière à s'assurer que le niveau de sécurité de ces derniers est périodiquement « *apprécié* » par les établissements eux-mêmes et que des actions correctives sont entreprises le cas échéant. De même, des procédures de secours informatiques doivent être « *disponibles* » afin d'assurer la continuité de l'exploitation en cas de difficulté grave dans le fonctionnement des systèmes informatiques [5].

Les établissements de crédit ont, en outre, pour obligation principale, de mettre en place un plan de continuité d'activité [6], lequel est défini comme un « *ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes de l'entreprise puis la reprise planifiée des activités* » [7].

De la même manière, le Règlement général de l'Autorité des marchés financiers (AMF) fait obligation aux sociétés de gestion d'établir et de maintenir opérationnels des plans de continuité de l'activité, afin de garantir la sauvegarde de leurs données et de leurs fonctions essentiel-

> *« Les établissements de crédit ne pourront se contenter d'arguer d'une faute de leur prestataire de services informatiques pour se décharger de tout ou partie de leur responsabilité à l'égard de leurs clients. »*

[2] Au plan international, les discussions engagées dans le cadre des accords de Bâle II. Au niveau européen, le groupe de travail CESR/SEBC (Comité des régulateurs européens de marchés de valeurs mobilières/Système européen de banques centrales) a tenté d'adapter les recommandations élaborées par le CPSS (Commitee on Payment and Settlement Systems), lequel regroupe les banques centrales du G10 et l'IOSCO (International Organisation of Securities Commissions) pour l'organisation, la sécurité et la surveillance des systèmes de compensation d'instruments financiers et des systèmes de règlement de titres ; et les réflexions engagées par les banques centrales de l'Eurosystème.

[3] Articles L. 533-2 et suivants du Code monétaire et financier.

[4] Article 14 du règlement n° 97-02 du CRBF.

[5] L'article 14 du règlement n° 97-02 CRBF rappelle par ailleurs que le contrôle des SI doit également permettre de s'assurer que l'intégrité et la confidentialité des informations sont assurées en toutes circonstances et qu'il s'étend à la conservation des informations et à la documentation relative aux analyses, à la programmation et à l'exécution des traitements.

[6] À noter qu'après le passage à l'an 2000, la notion de continuité telle qu'elle était appréhendée est apparue insuffisante face aux différents scénarios à envisager, et demeure une notion évolutive. Le règlement du CRBF n° 2004-02 du 8 janvier 2004 modifiant le règlement n° 97-02 du CRBF, a imposé la mise en place, dans tous les établissements, d'un plan de continuité des activités prenant en considération l'ensemble des infrastructures fonctionnelles ; « Le plan de continuité d'activité une assurance survie », Catherine Hazart, Banque et informatique, 1er mars 2003.

[7] Article 4n) du règlement n° 97-02 du CRBF.

1. NON-RESPECT DES OBLIGATIONS DE SÉCURITÉ DES SI

Les sanctions

La Commission bancaire exerce son contrôle à l'occasion du dépôt, par les entreprises assujetties, d'un rapport annuel qui doit décrire le projet ayant abouti au plan de continuité de l'activité, le plan lui-même, la répartition des responsabilités nécessaires à sa mise en œuvre ainsi, que les résultats des tests réalisés pour s'assurer de la continuité de l'exploitation en cas de survenance d'une crise [1]. Les sanctions applicables en cas de violation des dispositions réglementaires ou législatives régissant l'activité des établissements de crédit en la matière, relèvent de l'article L. 613-21 du Code monétaire et financier et peuvent aller de l'octroi d'un simple avertissement à la radiation de l'établissement [2].

Dans une décision rendue le 3 juillet 2008, la Commission bancaire a prononcé un blâme et une sanction pécuniaire de 4 millions d'euros à l'encontre d'un établissement de crédit en raison de divers manquements aux procédures de contrôle interne. Cette décision retient, s'agissant de la sécurité informatique, une non-conformité aux prescriptions de l'article 14a du règlement n° 97-02 prévoyant que les établissements de crédit ont pour obligation « *d'apprécier* » périodiquement le niveau de sécurité des systèmes informatiques et d'entreprendre, le cas échéant, les actions correctives nécessaires.

Retenant dans cette décision que la sécurité du SI de l'établissement bancaire concerné présentait des failles importantes ayant permis à un opérateur de « *créer, modifier et supprimer les opérations fictives utilisées pour dissimuler ses risques et ses résultats* », la Commission a décidé que l'infraction était établie. Cette décision met également en évidence le fait que l'un des risques majeurs contre lesquels les établissements de crédit doivent se prémunir est le risque de fraude, c'est-à-dire le risque opérationnel ou humain, le plus souvent également à l'origine des dysfonctionnements techniques des SI.

Dans sa décision plus récente du 15 juillet 2009, le blâme prononcé par la Commission bancaire est accompagné d'une sanction pécuniaire de 20 millions d'euros. Cette décision retient également une non-conformité aux prescriptions du règlement n° 97-02 du CRBF et en particulier, s'agissant de la sécurité des SI, à son article 14.

La Commission bancaire relève que les modalités du contrôle des habilitations informatiques étaient insuffisantes et que certains outils ne respectaient pas parfaitement les règles internes de sécurité relatives aux mots de passe prévues au niveau du groupe. La Commission fait donc une interprétation stricte de l'obligation posée à l'article 14 du règlement n° 97-02 du CRBF, lequel dispose que les entreprises assujetties déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leur métier mais que, une fois ce niveau retenu, et en l'espèce des règles internes validées au niveau du groupe, elles veillent à ce que le niveau retenu soit respecté, périodiquement « *apprécié* » et, le cas échéant, corrigé.

Là encore, on voit poindre en arrière-plan la nécessité de se prémunir contre les risques de fraude interne. À ce titre, il n'est pas inintéressant de noter que la 7e recommandation figurant dans le rapport Lagarde déposé au lendemain de l'affaire Kerviel, mentionnait précisément la nécessaire protection des codes d'accès

[1] Annexe à la lettre du Secrétaire général de la Commission bancaire au Directeur général de l'Association française des établissements de crédit et des entreprises d'investissement, rapport sur le contrôle interne en application de l'article 42 du règlement n° 97-02 du CRBF.

[2] Rapport annuel 2007 de la Commission bancaire, p. 10.

UN PLAN DE SECOURS GLOBAL

Le plus souvent, la mise en œuvre de cette obligation implique l'implantation de deux sites distants et la mise en place d'un mode de stockage et de sauvegarde des données par réplication, c'est-à-dire de manière simultanée sur chacun des deux sites, cette méthode ayant l'avantage d'assurer un risque quasi inexistant de perte d'information en cas de dysfonctionnement de l'un des sites seulement. Ce modèle s'est notamment développé sous l'influence des exigences de Bâle II, en abandonnant les plans de passage en secours, application par application, au profit d'un plan de secours global entre un centre informatique et son « clone » [10] situé sur un site distant.

En outre, les plans de continuité de l'activité mis en place doivent s'intégrer de façon cohérente à un plan plus global de sécurité défini par l'organe exécutif de l'établissement de crédit [11].

Les établissements de crédit ont également, au titre de l'article 15 du règlement n° 97-02 du CRBF, un certain nombre d'obligations à respecter en matière de conservation et d'archivage des données. Celles-ci ont également donné lieu à une évolution de la réglementation applicable aux prestataires de service d'investissement, rapprochant les règles applicables à ces derniers de celles relatives aux établissements de crédit [12].

Le renforcement de ces exigences réglementaires pesant sur les établissements de crédit s'est enfin traduit par l'apparition de fonctions spécialisées au sein des entités du secteur bancaire et financier, comme celles

les, en cas d'interruption de leurs systèmes et procédures, ainsi que la poursuite de leurs services d'investissement ou de gestion d'OPCVM [8]. En cas d'impossibilité de poursuite de ces services, le Règlement général de l'AMF prévoit que la société de gestion devra disposer d'un plan de continuité d'activité lui permettant la récupération en temps utile de ces données et fonctions et la reprise de ses activités. La même obligation pèse sur le teneur de compte conservateur [9].

[8] Article 313-56 du règlement général de l'AMF.

[9] Article 322-16 du règlement général de l'AMF.

[10] « Les plans de continuité d'activité, un élément important de Bâle II », Alain Dequier, *Banque Magazine* n° 647, mai 2003.

[11] Article 14-1c) du règlement n° 97-02 du CRBF.

[12] « Traçabilité et prestataires de services d'investissement - Élément de réflexion en matière de sécurité informatique concernant la transposition de la directive MIFID », E. Caprioli, *Revue de droit bancaire et financier*, juillet-août 2007.

2. DYSFONCTIONNEMENT DU SYSTÈME TÉLÉMATIQUE

Une jurisprudence remarquée

■ Dans une affaire récente, le titulaire d'un abonnement interactif accessible par Minitel pour la transmission d'ordres de bourse a mis en cause la responsabilité de sa banque en raison d'un dysfonctionnement du système télématique, invoquant dès lors une violation de la réglementation en matière de couverture d'ordres de bourse à règlement différé. L'appelant, qui avait été débouté en première instance en application d'une jurisprudence alors classique, invoquait les dysfonctionnements du serveur informatique lui ayant permis de passer des ordres de bourse sans couverture suffisante, en faisant valoir, outre le défaut de respect des règles de couverture des ordres à découvert, un manquement de la part de la banque à son devoir de conseil, d'information et de vigilance. La cour d'appel de Nîmes, accueillant dans un premier temps l'argument, l'a finalement écarté en rappelant que l'obligation de mise en garde pesant sur la banque s'apprécie en considération de la compétence et de l'expérience du client, excluant en l'espèce un manquement de la banque [1]. Toutefois, la cour d'appel a retenu la responsabilité de la banque pour manquement à ses obligations contractuelles, dès lors que la défaillance du système informatique avait pu causer un préjudice à son client et que la clause limitative de responsabilité contenue dans ses conditions générales de vente n'était pas opposable à ce dernier.

[1] Nîmes, Ch. civ. 1, section B, 4 mars 2008, n° 04/006 653.

de responsable du plan de continuité d'activité, ou de directeur de la conformité, lesquels sont garants du respect des lois et des règlements auprès des autorités de tutelle, et moteurs des projets informatiques nécessaires à la mise en conformité [13].

LA RESPONSABILITÉ DES ÉTABLISSEMENTS EN CAS DE DÉFAILLANCE DE LEUR SI

Face à l'impérative nécessité pour les établissements de crédit de s'adapter à des besoins toujours plus complexes en matière de SI, des entreprises de services spécialisées dans ce domaine se sont développées sur ce marché. La participation active de ces sociétés tierces [14] à la mise en conformité des SI des établissements de crédit, conduit à s'interroger sur le partage des responsabilités pouvant s'opérer entre les deux intervenants, dans l'hypothèse d'une défaillance du système informatique qui a pour origine un manquement à une obligation réglementaire dont le prestataire de services informatiques devait précisément assurer le respect.

La question se pose dans le cadre des relations contractuelles de l'établissement de crédit non seulement avec son prestataire de services informatiques, mais également avec ceux de ses propres clients auxquels cette défaillance aurait causé un préjudice.

...À L'ÉGARD DE LEURS CLIENTS

D'une façon générale, la question de responsabilité des établissements de crédit à l'égard de leurs clients en cas de dysfonctionnement de leurs systèmes informatiques est tranchée par la jurisprudence à la lumière de leurs obligations contractuelles et de leur devoir plus général de mise en garde et de conseil. Faut-il admettre, par ailleurs, que la responsabilité civile contractuelle des établissements de crédit pourrait être recherchée devant un juge en cas de manquement à leurs obligations réglementaires ?

En matière de services de bourse en ligne, à l'occasion d'opérations transmises par le biais d'internet ou d'un minitel, la jurisprudence a été amenée à traiter de la responsabilité des banques et des PSI en raison de la défaillance de leurs systèmes informatiques. Dans plusieurs cas d'espèce récents (*encadré* 2), des décisions sont venues rappeler que pèsent sur l'établissement de crédit deux types d'obligations :

– l'obligation de sécuriser ses systèmes informatiques et d'informer ses clients sur les risques inhérents à l'utilisation de ces systèmes ;

– l'obligation d'exécuter les services offerts conformément aux dispositions contractuelles applicables [15].

Dans ces décisions, afin de déterminer si la responsabilité de l'établissement de crédit est engagée, la jurisprudence fait une simple application des principes de la responsabilité contractuelle en recherchant la preuve d'une faute, d'un préjudice et d'un lien de causalité entre ladite faute et ledit préjudice [16].

En outre, à la lumière de ces cas d'espèces et des décisions récentes de la Cour de cassation relatives à la responsabilité du PSI pour défaut d'appel de couverture [17], il apparaît clairement une volonté de faire entrer les obligations réglementaires pesant sur les établissements de crédit et les PSI dans le champ contractuel de leurs relations avec leurs propres clients. Poussé à l'extrême, ce mouvement jurisprudentiel pourrait conduire à penser qu'en cas de violation par un établissement de crédit de ses obligations réglementaires, comme en cas de défaut de conformité du plan de continuité de l'activité de ce dernier, sa responsabilité contractuelle pourrait être engagée à l'égard de l'un de ses clients, si ce manquement lui avait causé un préjudice.

« La sécurité informatique fait partie intégrante du dispositif prudentiel des établissements de crédit. En ce sens, elle doit être comprise comme une composante du contrôle interne. »

[13] « Directeur de conformité Anticiper sur les risques », Cyril Vegni, Banque et informatique, 1er octobre 2008.

[14] Pouvant aller de la simple prestation de services à la création d'une société conjointe avec leur client, ayant pour objet exclusif la mise en place et la gestion du SI (création par exemple d'une *joint venture* entre BNP Paribas et IBM).

[15] Riom, Ch. com., 28 février 2007, n° 06/01 246 ; Paris, Ch. 15 section B, 23 juin 2006, n° 05/01 631.

[16] Pour des décisions n'ayant pas retenu de responsabilité de la banque en dépit du dysfonctionnement de son système informatique : Nancy, Ch. civ. 1, 1er octobre 2007 n° 05/00710 ; Nouméa, 4 janvier 2007, n° 05/527 ; Chambéry, Ch. com. 21 novembre 2006, n° 05/02 804. À l'inverse Paris, Ch. 15 section B, 15 septembre 2006, n° 05/04 243 ; Nîmes, Ch. civ. 1 section B, 4 mars 2008, n° 04/00653.

[17] Cass. Com 26 février 2008, n° 07-10 761 et Cass. Com. 4 novembre 2008, n° 07-27 481 et n° 07-21 449.

Par ailleurs, un établissement de crédit pourrait voir sa responsabilité engagée à l'égard d'un de ses clients, sur le fondement des articles L. 533-1 et L. 533-11 du Code monétaire et financier lui imposant d'agir d'une manière « *professionnelle* » favorisant l'intégrité du marché et servant au mieux les intérêts du client.

VERS UN PARTAGE DE RESPONSABILITÉ AVEC LES PRESTATAIRES DE SERVICE ?

Or, les établissements de crédit faisant de plus en plus volontiers appel à des prestataires de services informatiques pour se mettre en conformité avec les textes, il est légitime de s'interroger sur le fait de savoir si une partie de ce risque juridique pourrait être assumé par ces prestataires.

Par le biais du recours à des contrats d'infogérance, la totalité des infrastructures informatiques, la surveillance des réseaux et l'administration de la sécurité peut en effet être transférée à un prestataire externe : plans de continuité, politiques liées aux connexions internet, gestion des droits d'accès, etc. Il est également possible de mettre en place une solution intermédiaire visant un compromis entre l'externalisation et la maîtrise interne de la sécurité, les prestataires extérieurs intervenant en application de contrats d'infogérance sur une partie précise de la sécurité informatique, comme la supervision à distance de l'activité des réseaux et des risques que fait courir Internet aux SI, la collecte des informations, ou l'archivage et la sauvegarde des données.

L'externalisation de ce type d'activité est relativement nouvelle, car si elle a toujours été pratiquée par les banques pour leurs services informatiques de production, ces mêmes établissements de crédit ont longtemps traité des questions de sécurité des systèmes informatiques de manière plus réservée. Il semble toutefois que dans un contexte économique où les établissements de crédit et les entreprises d'investissement recherchent la productivité et la fidélisation de leurs clients, ces derniers tendent même à utiliser la voie de ce que certains appellent « l'externalisation globale » ou « l'infogérance globale » et se concentrent sur leurs métiers fondamentaux.

L'intérêt d'une telle solution pourrait reposer, à première vue, sur la possibilité de transférer la gestion de ces risques à un prestataire extérieur par le jeu de la rédaction des clauses contractuelles et, en particulier, de l'insertion de clauses limitatives de responsabilité. Toutefois, il convient de noter qu'il ressort de l'article 37-2 du règlement n° 97-02 du CRBF que « *les entreprises assujetties qui externalisent des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes, [...] demeurent pleinement responsables du respect de toutes les obligations qui leur incombent* ».

Le règlement n° 97-02 du CRBF dispose également que les dispositifs de contrôle visés à l'article 5 incluent les activités externalisées. Si l'on rappelle que cet article 5 dispose que le système de contrôle des opérations et des procédures internes a notamment pour objet de « *vérifier la qualité des SI et de communication* », la lecture combinée de cet article et de l'article 37-1-1 du même règlement amène à conclure très précisément que l'établissement de crédit doit se doter de moyens de contrôler, y compris son système informatique externalisé. L'ampleur de la responsabilité qui pèse alors sur les établissements de crédit dans le cadre de leurs obligations de contrôle interne ne s'arrête pas, par conséquent, aux portes de l'externalisation. Dès lors, les établissements de crédit ne pourront se contenter d'arguer d'une faute de leur prestataire de services informatiques pour se décharger de tout ou partie de leur responsabilité à l'égard de leurs clients, et ce d'autant plus que les éventuelles clauses limitatives de responsabilité négociées par les établissements de crédit avec leurs prestataires informatiques leur sont inopposables.

...À CONDITION D'UNE RÉDACTION RIGOUREUSE DES CONTRATS

En dépit de ce contexte réglementaire, il ne peut être exclu que la responsabilité des prestataires de services informatiques puisse être recherchée, le cas échéant, à tout le moins dans le cadre d'un appel en garantie ou d'une intervention forcée. À ce titre, il conviendra, pour les établissements de crédit, de veiller à la rédaction rigoureuse des clauses de leurs contrats, en s'assurant de la précision des engagements pris par les prestataires de services informatiques, par le biais notamment d'obligations de résultat ou de moyen renforcées. En effet, pour que les établissements de crédit et les entreprises d'investissement puissent se retourner contre leurs prestataires, encore faudra-t-il que les obligations réglementaires auxquelles ils sont soumis soient entrées dans le champ des relations contractuelles qui les lient avec ces derniers.

Enfin, pour éviter que les prestataires de services informatiques ne fassent jouer trop aisément des clauses limitatives de responsabilité dont la validité est admise par les tribunaux, il pourra être prudent de veiller à ce que le contrat de prestations de services informatiques mette expressément à la charge du prestataire l'obligation essentielle d'avoir à assumer le respect de leurs obligations réglementaires par les établissements de crédit. ■