Cybersécurité : notifications des incidents de sécurité

SABINE MARCELLIN*

Juriste d'entreprise

Face à l'évolution incontestable des cyber-risques, les organisations s'adaptent. La règlementation évolue fortement pour renforcer la sécurité des systèmes d'information. Pour les banques, à côté de mesures réglementaires déjà intégrées, de nouvelles obligations apparaissent. Parmi ces obligations figure la notification des incidents de sécurité, pratiquée dans différents pays. Quels sont les textes législatifs et réglementaires imposant cette notification ? Auprès de quels interlocuteurs les incidents devront-ils être notifiés ? Quelles sont les conséquences opérationnelles pour les établissements financiers ?

La sécurité des systèmes d'information est un enjeu majeur pour les établissements financiers. Les objectifs de sécurité sont d'assurer la disponibilité, l'intégrité, la confidentialité et le caractère probant des données traitées.

Les moyens de prévention majeurs reposent sur l'*élaboration d*'une politique de sécurité, la gestion des habilitations, l'application de règles d'utilisation, la sensibilisation et formation et la surveillance des systèmes. Parmi les moyens de surveillance, figure déjà le recensement et l'analyse des incidents de sécurité. Il existe des structures dans les organisations publiques et privées, dont les banques, connues sous les acronymes de SOC, CERT ou CSIRT[1] dont le rôle est de centraliser les demandes d'assistance suite aux incidents de sécurité, de traiter les alertes, d'*établir* une base des vulnérabilités et de prévenir par diffusion d'informations et de se coordonner avec les autres acteurs.

En France, aujourd'hui, la notification d'incidents devient une obligation. Les organisations devront faire connaître à des régulateurs publics, voire aux personnes concernées, l'existence d'incidents touchant des données ou réseaux. Cette obligation existe déjà dans notre pays pour les opérateurs de communication électronique, depuis 2011.

Plus globalement, cette obligation devrait s'*étendre, portée par plusieurs projets législatifs français et européens visant à renforcer la cybersécurité.*

Comment cette tendance forte, venue d'Outre-Atlantique, se décline dans les projets législatifs et réglementaires ? Quelles sont les questions juridiques soulevées[2] *et les conséquences opérationnelles pour les entreprises et organisations ?* Comment les banques doivent-elles intégrer ces futures *règles ?*

Concept de notification d'incidents de sécurité

Un incident de sécurité peut être défini[3] comme un *événement* intéressant la sécurité de l'information, qui est indésirable ou inattendu, et présente une probabilité forte de menacer la sécurité de l'information et de compromettre les opérations liées à l'activité de l'organisation.

La surveillance des incidents est une pratique déjà existante. La « notification » d'un incident signifie qu'il est porté à la connaissance d'un tiers. Au plan juridique, les différents textes ou propositions ne définissent pas stricto sensu la notion de notification. Il est question, cependant, de porter l'incident à la connaissance de l'autorité

* Les propos développés dans cet article correspondent à l'approche personnelle de l'auteur et ne sauraient représenter l'opinion de l'entreprise, ni du groupe au sein desquels elle exerce.

1. *Security Operation Center*, *Computer Emergency Response Team* et *Computer Security Incidence Response Team*. Consulter le site de l'Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr).

2. Consulter « Notifications des incidents – FAQ » publié en juillet 2014, sur le site du Forum des Compétences, association d'établissements financiers ayant pour objet la coopération en matière de sécurité de l'information. Ce FAQ a été élaboré avec l'assistance du cabinet d'avocats Caprioli & Associés.

3. D'après les normes ISO/CEI 27001 Technologies de l'information –Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences et ISO/CEI 27002 Code de bonnes pratiques pour la gestion de la sécurité de l'information.

Tableau n° 1 - Pays disposant d'une réglementation générale relative aux notifications
Allemagne
Autriche
Corée du Sud
Danemark
États-Unis (48 États)
Italie
Mexique
Norvège
Philippines
Uruguay

Source : DataGuidance, août 2014

de contrôle ou de la personne concernée.

En pratique, plusieurs termes synonymes sont employés pour désigner cette même réalité juridique comme « avertir », « communiquer » ou « alerter ».

L'objectif premier de la notification est opérationnel. Elle permet à un organisme d'identifier une attaque ou un comportement malveillant et d'anticiper les moyens de réaction organisationnels adaptés selon l'évaluation de l'impact potentiel. Plus largement, la notification va permettre une communication maîtrisée de l'incident, en l'insérant dans un contexte géopolitique ou socioéconomique. L'analyse des incidents permet d'identifier des schémas techniques ou comportementaux et ainsi d'anticiper l'origine de dysfonctionnements. La notification à large échelle, dans un souci de visibilité et d'établissement de statistiques fiables permet, selon l'ENISA, une action concertée et efficace des règles de sécurité[4].

Nous nous intéresserons d'une part à l'évolution législative et réglementaire (I) et d'autre part aux questions soulevées par la mise en œuvre des notifications des incidents de sécurité (II).

I. ÉVOLUTION LÉGISLATIVE

La notification d'incidents visant à éviter les usurpations d'identité s'est développée, depuis 2002[5], dans la quasi-totalité des États américains. D'autres pays ont intégré dans leur législation une obligation de notification (voir Tableau n° 1). La notification est globale dans certains États ou applicable à certains domaines de la sécurité de l'information afin d'inciter à la sécurisation des systèmes et de recenser l'*évolution de certains phénomènes de cybercriminalité*, comme pour l'Australie ou l'Inde.

Au sein de l'Union européenne, certains États membres ont adopté des textes généraux, comme l'Allemagne, l'Autriche, le Danemark ou l'Italie. D'autres États membres disposent de textes législatifs relatifs à la notification applicables à des secteurs particuliers, comme la Grèce, la Suède ou la France.

La première notification obligatoire apparaît en France en 2011[6], lors d'une réforme de la loi dite « *informatique et libertés* »[7], et s'applique aux prestataires de services de communications électroniques. Ces prestataires doivent notifier auprès de la CNIL les incidents de sécurité relatifs aux données personnelles et dans certains cas, notifier également les incidents auprès des personnes concernées. Qui sont les entreprises visées par l'appellation « *prestataires de services de communications électroniques* » ? Au-delà des opérateurs de télécommunications et des fournisseurs d'accès à Internet (p. ex : Orange, SFR, Bouygues, Free, etc.), ces prestataires sont définis comme les entreprises qui proposent des « *prestations consistant entièrement ou principalement en la fourniture de communications électroniques. Ne sont pas visés les services consistant à éditer ou à distribuer des services de communication au public par voie électronique* »[8] (p. ex : Facebook, etc.).

À la date de publication du présent article, plus de 1 600 opérateurs sont déclarés auprès de l'Autorité de régulation de communication électronique et des postes (ARCEP)[9].

Le mécanisme de notification semble appeler à se développer au sein d'autres dispositifs juridiques. Différents projets de textes législatifs européens et français traitent de la notification des incidents de sécurité.

Textes et projets réglementaires européens

À Bruxelles, parmi les projets en cours, plusieurs textes intègrent dans leurs dispositions l'obligation de notification[10]. Face à l'*évolution des technologies, il semble nécessaire* d'adapter et de renforcer l'harmonisation de la sécurité de l'information. Un règlement adopté en juillet 2014 (1.) comprend déjà le principe de notification et trois projets (un règlement et deux directives) pouvant intéresser le secteur bancaire (2.) sont brièvement repris ici.

1. Un règlement européen comprend le principe de notification

Le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques a été adopté le 23 juillet 2014[11]. Ce texte, dit PSC ou eIDAS, vise à garantir l'existence de transactions électroniques transnationales efficaces et sûres. Il représente la volonté de créer « *un socle commun pour des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques* ».

4. « Les notifications de violations de données en Europe », ENISA – European Networks and Information Security Agency, janvier 2011, enisa.europa.eu.
5. « *Senate Bill 1386* » du 12 février 2002, entré en vigueur le 1er juillet 2003, et introduisant dans le Code civil californien des dispositions imposant la révélation des incidents de sécurité.
6. Ordonnance n° 2011-1012 du 24 août 2011 applicable depuis le 27 août 2011 à l'exception des dispositions subordonnées à la publication d'un décret ou arrêté.
7. Article 34 bis de la loi n° 78-17 modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et décret n° 2012-436 du 30 mars 2012.
8. Article L. 32, alinéa 6, du Code des postes et des communications électroniques.
9. ARCEP – liste à consulter sur « arcep.fr ».
10. « Obligation de notification des failles de sécurité : quand l'Union Européenne voit double », François Coupez, octobre 2010 (juriscom.net).
11. Règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

Le règlement fixe naturellement des exigences de sécurité applicables aux prestataires de services de confiance, dans son article 19. Parmi les exigences figure l'obligation de notification d'atteinte à la sécurité, auprès de l'organe de contrôle et, le cas échéant, *« à d'autres organismes concernés, tels que l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données ». De plus, lorsque* l'atteinte à la sécurité concerne deux États membres ou plus, « l'*organe de contrôle notifié informe les organes de contrôle des autres États membres concernés ainsi que* l'ENISA[12]. » Le règlement sera applicable le 1er juillet 2016, sauf certaines dispositions déjà en vigueur depuis le 17 septembre 2014. Les dispositions relatives aux notifications ne sont pas applicables à ce stade. D'ici là, la Commission européenne a la possibilité de définir, au moyen d'actes d'exécution, les formats et procédures, y compris les délais de ces notifications. La mise en œuvre de la procédure de notifications auprès de différentes autorités de tutelle nécessite, en amont, un important travail de coordination, tant entre les instances nationales qu'au niveau européen.

2. Trois projets de textes traitent de notification d'incidents

La proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dans sa version du 25 janvier 2012[13], a pour objet de réformer les règles applicables aux données personnelles. La directive applicable actuellement a été adoptée en 24 octobre 1995 et transposée dans tous les États membres.

La proposition de règlement a été adoptée par la Commission LIBE[14] le 21 octobre 2013 et elle a été également soutenue par le Conseil européen des 24 et 25 octobre 2013. Une version du règlement a été adoptée en première lecture par le Parlement européen le 12 mars 2014. Parmi les évolutions majeures prévues : un renforcement de la coopération entre les agences nationales de protection des données, la nomination d'un correspondant aux données dans les entreprises d'une certaine taille et des dispositions de notification d'incidents de sécurité relatifs aux données personnelles. La proposition prévoit que tous les États membres rendent obligatoire la notification d'incidents relatifs à des traitements de données personnelles auprès des agences de protection des données des États membres, comme la CNIL en France, et que, dans certains cas, une information des personnes concernées par l'incident soit obligatoire. Le 17 septembre 2014, une position commune de représentants de parlements nationaux a été publiée (soit dix pays : Allemagne, Autriche, Belgique, Croatie, France, Grèce, Italie, Luxembourg, Roumanie et Lituanie). Ils soutiennent l'adoption de règles européennes, notamment le mécanisme de guichet unique et l'application uniforme des règles. Ils estiment nécessaire l'adoption, d'ici 2015, d'un cadre permettant de « *garantir le respect du droit fondamental à la protection des données et d'imposer [...] les valeurs européennes en matière de protection et de sécurité des données personnelles* ».

Le 26 septembre 2014, le Conseil de l'Union européenne a également suggéré des modifications relatives à la notification (cf. considérants 67, 68 et 69, et cf. article 31).

Un autre texte est à citer. Il s'agit de la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union – 2013/048 (dite SRI ou NIS). Le texte a été adopté par le Parlement européen le 13 mars 2014 en première lecture. Son objectif est d'améliorer le niveau de sécurité des réseaux et systèmes informatiques privés sur lesquels reposent les services dont dépend le fonctionnement de la société dans l'UE. Cette proposition de directive démontre une volonté des États membres d'améliorer leur niveau de préparation et leur coopération mutuelle. C'est une incitation à la mise en place de mesures appropriées pour les opérateurs d'infrastructures critiques et les administrations publiques, afin de gérer les risques de sécurité et de signaler les incidents graves aux autorités nationales compétentes.

La proposition prévoit des obligations à la charge des opérateurs d'infrastructures critiques qui sont similaires à celles issues de la loi de programmation militaire pour les opérateurs d'importance vitale, examinées ci-après.

Par ailleurs, une autre proposition de directive est à signaler, concernant les services de paiement dans le marché intérieur[15]. Elle est dite DSP2 ou PSD2, et sa dernière version a été publiée le 24 juillet 2013. Elle vise à remplacer la directive sur les services de paiement DSP1, mise en œuvre par les États membres au 1er novembre 2009. Le 24 juillet 2013, la Commission européenne a publié deux propositions : une directive qui abrogera la DSP1 et un règlement sur les commissions d'interchange pour les transactions de paiement par carte.

Les principaux projets réglementaires européens qui contiennent des dispositions relatives à la notification des incidents de sécurité sont recensés dans le Tableau n° 2.

Textes et projets réglementaires en France

La loi de programmation militaire du 18 décembre 2013[16] (LPM) a pour objectif l'organisation de la défense et la sécurité nationale pour les années 2014 à 2019. Parmi de nombreux dispositifs relatifs à la défense nationale, ce texte introduit des mesures générales de sécurité des systèmes d'information pour les opérateurs d'importance vitale (OIV).

La LPM a été un véhicule puissant pour élargir les obligations des OIV, jusque-là centrées sur la sûreté des infrastructures, à la sécurité des systèmes d'information. La notification ne constitue que l'une des obligations parmi d'autres.

Afin de garantir la survie de la nation, la LPM introduit de nouvelles obligations pour les OIV applicables à la

12. European Network and Information Security Agency.
13. Référencée 2012/0011.
14. Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen.
15. La proposition modifie les directives 2002/65/CE, 2013/36/UE et 2009/110/ CE et abroge la directive 2007/64/CE – 2013/264.
16. Loi n° 2013-1168 de programmation militaire du 13 décembre 2013 et décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale.

Tableau n° 2 - Projets réglementaires européens incluant des dispositifs de notification d'incidents

Texte	Date	Objet
Proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - 2012/0011 (règlement général sur la protection des données)	25 janvier 2012 (dernière version)	Réforme de la directive existante (24 octobre 1995) face à l'évolution des technologies pour renforcer l'harmonisation de la protection des données à caractère personnel.
Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union – 2013/048 (dite SRI)	13 mars 2014 (adoption en première lecture)	Améliorer le niveau de sécurité des réseaux et systèmes informatiques privés sur lesquels reposent les services dont dépend le fonctionnement de la société dans l'Union européenne. Volonté que les États membres améliorent leur niveau de préparation et leur coopération mutuelle. Incitation à la mise en place de mesures appropriées pour les opérateurs d'infrastructures critiques et les administrations publiques, afin de gérer les risques de sécurité et signaler les incidents graves aux autorités nationales compétentes.
Proposition de directive concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/UE et 2009/110/CE et abrogeant la directive 2007/64/CE – 2013/264 (dite DSP2 ou PSD2)	24 juillet 2013 (dernière version)	Remplacement de la directive sur les services de paiement DSP1, mise en œuvre par les États membres au 1er novembre 2009. Le 24 juillet 2013, la Commission européenne a publié deux propositions : une directive qui abrogera la DSP1 et un règlement sur les commissions d'interchange pour les transactions de paiement par carte.

sécurité des systèmes d'information : accès au système d'information (SI) par l'ANSSI, mise en œuvre de systèmes qualifiés de détection d'événements susceptibles d'affecter la sécurité du SI, notification de failles et contrôles de la sécurité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Ce texte s'applique exclusivement aux OIV, c'est-à-dire des entreprises et administrations désignées comme telles par l'instruction générale du 7 janvier 2014[17]. Cette instruction organise un dispositif de Sécurité des activités d'importance vitale (SAIV) qui est inséré dans le Code de la défense, notamment ses articles R. 1332-1 à 1332-42, pris sur le fondement de ses articles L. 1332-1 à 1332-7. Ce dispositif constitue le cadre législatif et réglementaire permettant d'associer les OIV, publics ou privés, au système national de protection contre le terrorisme, le sabotage et les actes de malveillance, d'analyser les risques et d'appliquer les mesures de leur niveau en cohérence avec les décisions des Pouvoirs publics.

L'instruction réforme en profondeur et unifie les dispositifs antérieurs applicables aux installations d'importance vitale. Elle s'inscrit plus largement dans une démarche d'ensemble visant à adapter les conditions dans lesquelles la nation se prémunit contre toute menace, notamment la menace terroriste.

La liste des OIV n'est pas publique ; il s'agit d'une information protégée par le secret de la défense. Les textes publics[18] nous permettent cependant de savoir que douze secteurs sont concernés : activités civiles de l'État, activités militaires de l'État, activités judiciaires, alimentation, communications électroniques et audiovisuelles, secteur de l'information, énergie, espace et recherche, finances, gestion de l'eau, industrie, santé et transport. Le tableau n° 3 présente les secteurs d'activité et leurs ministres coordinateurs.

Le nombre d'OIV serait de 218 en janvier 2014[19]. Certains établissements financiers sont des OIV.

Dans la LPM, nous examinerons le chapitre IV qui contient les « *dispositions relatives à la protection des infrastructures vitales contre la cybermenace* ». Ce chapitre crée ou fait évoluer différents articles dans le Code de la défense, le Code de propriété intellectuelle et le Code des postes et communications électroniques. Il vise à renforcer le dialogue public/privé dans la lutte contre la cybercriminalité.

Ces dispositions sont formalisées dans les articles présentés ci-après.

L'article 21 insère une disposition reconnaissant que l'ANSSI est placée sous l'autorité du Premier ministre et assure la fonction d'Autorité nationale de défense des systèmes d'information.

Ce même article 21 indique, que pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État « *peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque* ».

Pour être en mesure de répondre à ces attaques, l'ANSSI

17. Instruction générale relative à la sécurité des activités d'importance vitale n° 660/SGDSN/PSE/PSN du 7 janvier 2014, qui annule et remplace l'instruction n° 660/SGDSN/PSE/PPS du 26 septembre 2008.

18. Arrêté du 2 juin 2006 fixant la liste des secteurs d'activité d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.

19. « L'ANSSI cyberprotège 218 opérateurs d'importance vitale », *La Voix du Nord*, 22 janvier 2014.

Tableau n° 3 - Annexe à l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activité d'importance vitale et désignant les ministres coordinateurs	
SECTEURS	**MINISTRES COORDONNATEURS**
Activités civiles de l'État	Ministre de l'intérieur
Activités judiciaires	Ministre de la justice
Activités militaires de l'État	Ministre de la défense
Alimentation	Ministre chargé de l'agriculture
Communications électroniques, audiovisuel et information	Ministre chargé des communications électroniques
Énergie	Ministre chargé de l'industrie
Espace et recherche	Ministre chargé de la recherche
Finances	Ministre chargé de l'économie et des finances
Gestion de l'eau	Ministre chargé de l'écologie
Industrie	Ministre chargé de l'industrie
Santé	Ministre chargé de la santé
Transports	Ministre chargé des transports

peut détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation de sa mission.

Les dispositions de sécurité de l'information sont formalisées dans l'article 22, indiquant que l'ANSSI fixe les règles de sécurité aux OIV et « *aux opérateurs qui participent à ces systèmes* ». Ces règles, que les opérateurs sont tenus d'appliquer à leurs frais, sont les suivantes :

– mettre en œuvre des systèmes de détection des événements susceptibles d'affecter la sécurité des systèmes, systèmes exploités par l'ANSSI et les prestataires de services qualifiés de l'ANSSI ;

– soumettre à des contrôles leurs systèmes d'information afin de vérifier le niveau de sécurité et le respect des règles de sécurité, ces contrôles étant effectués par l'ANSSI ou des prestataires qualifiés par l'agence ;

– notifier les incidents de sécurité auprès de l'ANSSI ;

– en cas de crise majeure, l'ANSSI peut décider des mesures que les OIV doivent mettre en œuvre.

Ce même article 22 dispose que les informations transmises à l'administration restent confidentielles et ajoute un article L. 1332-6-5 dans le Code de la défense. Enfin, il introduit le cadre des sanctions, sur lesquelles nous reviendrons ci-après, et annonce un décret d'application.

L'article 23 introduit une modification de l'article 226-3 du Code pénal, afin de permettre à l'ANSSI, dans le cadre de ses missions de sécurité des systèmes d'information d'utiliser des appareils pour intercepter des informations sur les réseaux, également appelés sondes.

L'article 24 permet également à l'Agence, pour les besoins de sa mission, d'obtenir des opérateurs de communications électroniques des informations relatives aux « *utilisateurs ou détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leurs systèmes.* » Pour être applicable, cet article 24 entraîne des modifications de dispositions du Code pénal, du Code des postes et télécommunications électroniques et du Code de la propriété intellectuelle.

Le dernier article du chapitre IV (25) prévoit aussi les conditions légales d'intervention de l'ANSSI. Pour cela, il aménage d'une part l'article 323-1 du Code pénal pour permettre à l'Agence d'utiliser tout équipement, logiciel ou données dans le cadre de son action, et d'autre part, l'article L. 122-6 du Code de la propriété intellectuelle pour autoriser la décompilation de logiciel par l'ANSSI afin d'en tester la sécurité.

Sanctions

La LPM, dans son chapitre IV consacré aux dispositions relatives à la protection des infrastructures vitales contre la cybermenace, introduit des sanctions pénales spécifiques, applicables au cas où les obligations énoncées ne seraient pas appliquées. Selon l'article 22 de la LPM, ces sanctions complètent l'article L. 132-6-1 du Code de la défense qui s'applique à la fois aux dirigeants des OIV et aux sociétés qualifiées d'OIV. Elles sont respectivement d'une amende de 150 000 euros pour les dirigeants qui ne satisferaient pas aux obligations spécifiées et de 750 000 euros pour les personnes morales.

Certains commentateurs ont considéré que le montant de ces sanctions était relativement faible comparé à d'autres domaines. Cependant, le choix du législateur de prévoir des sanctions pénales à la fois pour les entreprises et leurs dirigeants semble incitatif à la mise en œuvre des mesures. S'agissant des failles de sécurité concernant des données personnelles, l'article 226-17-1 du Code pénal sanctionne l'absence de notification à la CNIL de cinq ans d'emprisonnement et d'une amende de 300 000 euros, ce chiffre étant multiplié par cinq pour les personnes morales. En outre, la CNIL dispose d'un pouvoir de sanctions administratives, notamment d'amendes et de publication de ses décisions.

De plus, est-il nécessaire de rappeler que la jurisprudence énonce qu'un traitement de données à caractère personnel non conforme à la loi n° 78-17[20] ne peut être pas vendu ni cédé ?

20. Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique et aux libertés.

1. Panorama des obligations de sécurisation de l'information dans le secteur bancaire

■ Outre les projets relatifs aux notifications d'incidents de sécurité, les banques sont déjà soumises à un ensemble de dispositifs réglementaires visant à renforcer la sécurité de l'information. L'obligation de sécuriser les informations personnelles est applicable depuis la loi dite « informatique et libertés » du 6 janvier 1978 à toutes les entreprises, les banques disposent d'un corps de règles spécifiques, visant à assurer le secret bancaire et plus largement la sécurité de l'information.

Une synthèse des différentes obligations applicables a été produite en 2011 par Le Forum des Compétences pour accéder facilement aux textes législatifs et réglementaires majeurs et cette publication est en cours d'actualisation[1].

Rappelons ici les obligations majeures à la charge des établissements financiers. Historiquement, la première source d'obligations relatives à la sécurité de l'information propre aux banques est le Règlement n° 97-02 du 21 février 1997 modifié, relatif au contrôle interne des établissements de crédit et des entreprises d'investissement, identifié le plus souvent par « le règlement 97-02 ». Ce texte a été rénové et remplacé par l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumis au contrôle prudentiel de l'Autorité de Contrôle Prudentiel (ACPR). Ce règlement oblige notamment les établissements à mettre en œuvre un plan de continuité d'activité et à sécuriser leurs systèmes d'information, en élaborant et appliquant des manuels de procédures. L'article 14 de l'arrêté indique que les entreprises assujetties « déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Elles veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés. » Les sanctions encourues peuvent aller de l'avertissement au retrait d'agrément, en passant par la démission d'office de dirigeants. Une sanction pécuniaire est possible également, jusqu'au décuple du capital minimum auquel est astreint l'établissement, ainsi qu'une publication de la sanction prise.

Par ailleurs, le règlement général de l'Autorité des marchés financiers (AMF), applicable aux entreprises offrant une prestation de teneur de compte conservateur, contient des dispositions en matière informatique, dans son Livre III, Titre II, chapitre II, article 322-12 et suivants. Ce règlement contient des dispositions applicables à la sécurité de l'information, dans les articles 322-12 et suivants, et impose notamment aux établissements assujettis de mener des analyses de risque pour déterminer le niveau souhaité de sécurité, d'établir une politique des habilitations d'accès aux systèmes et de formaliser la documentation du système d'information, d'établir une politique de sécurité physique et de continuité d'activité. Parmi ces mesures, figure également, dans l'article 322-15 l'obligation de mise en place d'indicateurs de suivi de la qualité et la sécurité de la production informatique, ainsi qu'un suivi des incidents avec leur gravité, leur origine et leur plan d'éradication.

Le Code monétaire et financier (CMF) créé en décembre 2000 rassemble les dispositions législatives et réglementaires applicables aux prestataires d'investissement et aux établissements de crédits. Le CMF impose à ces acteurs financiers de disposer de dispositifs efficaces d'évaluation des risques et de contrôle des systèmes informatiques. Pour les établissements de crédit, le CMF confie au ministre chargé de l'économie la charge d'arrêter les règles relatives à ces dispositifs. C'est l'objet de l'arrêté du 3 novembre 2014 évoqué ci-dessus. Enfin, pour les prestataires de services de paiement, le CMF impose d'assurer la sécurité des moyens d'authentification offerts aux utilisateurs de ces services.

Au niveau européen, il faut signaler également la publication de recommandations concernant la sécurité des paiements sur internet par la Banque centrale européenne, le 1er février 2013. Pour protéger l'initiation des paiements en ligne et les données sensibles, les recommandations incitent à la mise en œuvre de mécanismes de surveillance, de multiples niveaux de sécurité et d'assistance aux clients. Ces Recommandations qui, sous le nouveau nom d'Orientations (Guidelines) relèvent désormais de la responsabilité de l'Autorité bancaire européenne seront applicables à compter 1er août 2015.

Les services de paiement ont intégré aussi PCI DSS. Il ne s'agit pas ici d'une obligation légale, mais d'une norme visant à renforcer la sécurité des données chez les fournisseurs de services de paiement par carte. Cette norme PCI DSS (Payment Card Industry Data Security Standard) a été développée par le PCI Security Standard Council qui réunit les principaux réseaux émetteurs de cartes (Visa, MasterCard, American Express, Discover et JCB). Les établissements financiers fournissant des services de paiement par carte appliquent la version 2.0 de cette norme depuis le 1er janvier 2011.

En fait, depuis le 1er janvier 2014, la nouvelle norme PCI-DSS v3.0 de novembre 2013 peut être utilisée pour la certification. Mais son ancienne version (v2.0) peut encore être utilisée jusqu'au 31 décembre 2014. Au 1er janvier 2015, c'est la v3.0 qui devient obligatoire.

Au-delà des textes strictement applicables à la sécurité dans la sphère financière, les acteurs financiers sont naturellement soumis à toutes les règles de droit commun générant directement ou indirectement une obligation de confidentialité : respect de la vie privée, secret des correspondances, etc.

1. Publication annoncée pour octobre 2015 (forum-des-competences.org).

Le contrat de vente ne serait pas licite[21]. L'arrêt en question du 25 juin 2013 trouve un écho dans l'étude annuelle 2014 du Conseil d'État intitulée « Le numérique et les droits fondamentaux »[22]. L'étude propose cinquante mesures et dans l'une d'elles[23], le Conseil d'État propose de « *codifier dans la loi la jurisprudence relative à la nullité des transactions portant sur des fichiers non déclarés ou non autorisés à la CNIL.* »

Avec la proposition de règlement européen du 25 janvier 2012, les amendes pourraient a priori monter jusqu'à 5 % du chiffre d'affaires annuel mondial d'une entreprise (article 79) ou 100 millions d'euros, le montant le plus élevé étant retenu.

En matière de notification des incidents de sécurité, les propositions de directives SRI, DSP 2 et la proposition de règlement eIDAS prévoient qu'il reviendra aux États membres de fixer les sanctions applicables en cas de non-respect de la directive, les sanctions devant être « *effectives, proportionnées et dissuasives* ».

21. Arrêt du 25 juin 2013, Cour de cassation, Chambre commerciale (n° 12-17.037).
22. Étude annuelle 2014 du Conseil d'État, « Le numérique et les droits fondamentaux », septembre 2014, La documentation française.
23. Proposition n° 20 « *porter une attention particulière aux transmissions de données personnelles d'une entité à une autre* [...] ».

II. QUELQUES QUESTIONS SOULEVÉES PAR LES NOTIFICATIONS

La mise en œuvre des mécanismes de notification répond à des objectifs louables de renforcement de la sécurité des systèmes d'information, de continuité d'activité et de maintien de la confiance. Cependant, dans l'intérêt des établissements financiers et dans l'intérêt collectif, un certain nombre de questions restent à traiter pour optimiser le dispositif.

Facteurs déclencheurs de notification

Dans les différents textes et projets relevés, les facteurs déclencheurs d'une notification diffèrent en fonction de l'obligation de notification concernée.

Pour la CNIL, toute violation de données à caractère personnel, même de gravité négligeable, devrait être, en théorie, notifiée[24] à l'autorité de contrôle.

La proposition de règlement européen sur la protection des données à caractère personnel ne les précise pas, mais l'*état de la proposition adoptée par le Parlement européen le 12 mars* 2014 indique que « *le comité européen de la protection des données est chargé d'émettre des lignes directrices, recommandations et bonnes pratiques [...] aux fins de l'établissement de la violation de données et de la détermination du retard injustifié [...] et concernant les circonstances particulières dans lesquelles un responsable du traitement et un sous-traitant sont tenus de notifier la violation de données à caractère personnel ». Le considérant 8 du règlement 611/2013 du 24 juin 2013* concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE modifiée, d'ores et déjà applicable, tente, en l'absence d'autres précisions dans le texte, de préciser le moment à partir duquel on est en juridiquement présence d'une violation de données à caractère personnel à notifier : « *le fait de simplement soupçonner qu'une violation de données à caractère personnel s'est produite ou de simplement constater un incident sans disposer d'informations suffisantes, malgré tous les efforts déployés à cette fin par un fournisseur, ne permet pas de considérer qu'une telle violation a été constatée aux fins du présent règlement* ».

Par ailleurs, en matière de notification des incidents réseaux, dans la directive SRI, le facteur déclencheur semble être l'impact « *significatif* » de l'incident sur le système de l'entité ou les services fournis. La version adoptée par le Parlement de la proposition de cette directive précise qu'« *afin de déterminer l'ampleur de l'impact d'un incident, il est, entre autres, tenu compte des paramètres suivants : nombre d'utilisateurs concernés, durée de l'incident et portée géographique* ».

Pour la LPM, les notifications s'appliqueront aux incidents importants relatifs aux systèmes critiques des OIV. Seuls les arrêtés en cours de préparation pourront définir précisément le contour des obligations.

Modalités de notification

La décision de notifier doit résulter de la concertation de différents services de l'entreprise amenés à avoir un rôle actif dans cette notification, et notamment les responsables de la sécurité de l'information, de la conformité, de la fonction juridique, de la communication et l'équipe gérant les données à caractère personnel. Une approche pluridisciplinaire est nécessaire pour coordonner les différents enjeux : qualification de l'incident, nécessité d'une notification, contact avec le régulateur concerné, contenu de la notification, conséquences juridiques et en termes d'image.

La responsabilité de l'établissement quant à la gestion des notifications nécessite donc la mise en place d'une organisation interne, adaptée aux caractéristiques de celui-ci et regroupant les différents acteurs au sein d'une cellule de crise. Cette cellule doit disposer d'un pouvoir de décision, afin de pouvoir déclencher la notification et être en lien direct vers un acteur du comité exécutif de l'entreprise. Elle pourra ainsi être en mesure de décider des moyens matériels, humains et financiers nécessaires à la résolution de l'incident et au respect des obligations de communication.

Quant au contenu de la notification, actuellement, seuls les textes[25] relatifs à la notification des violations de données à caractère personnel en précisent les éléments.

Il ressort de ces différents textes[26] que la notification à la CNIL doit contenir notamment :

– la nature et les conséquences de la violation des données à caractère personnel ;

– les mesures déjà prises ou proposées pour y remédier ;

– le nombre de personnes concernées par la violation.

En matière d'incidents réseaux, si l'article D. 98-5 du Code des postes et communications électroniques ne précise pas les éléments contenus dans la notification, il précise les informations qui seront à fournir par l'opérateur après analyse de l'incident, à savoir les causes et conséquences des atteintes à la sécurité et les mesures prises.

La LPM ne définit pas les modalités de la notification, celles-ci devant *a priori* l'être dans un décret ou un arrêté.

Comme une notification aboutissant à une information du public peut avoir un impact non négligeable sur l'image de l'entreprise concernée, il est souhaitable de coordonner la communication au public avec l'autorité en charge de l'instruction de la notification. Ainsi, la cellule de crise aura notamment pour tâche de coordonner ces échanges et d'adopter le plan de communication associé à cette notification, en intégrant les exigences légales applicables en matière de communication.

Au plan européen, la proposition de règlement européen relatif aux données personnelles précise quelques informations supplémentaires, à savoir les catégories et le nombre d'enregistrements de données concernés et les mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données. La notification aux personnes intéressées doit quant à elle contenir des informations détaillées, en utilisant un langage clair et simple.

La directive n° 910/2014 précitée relative aux prestataires de services de confiance ne précise pas les informations que doit contenir la notification, mais prévoit que la Com-

24. Délibération n° 2013-358 de la CNIL et formulaire de notification de violation de données à caractère personnel publié sur son site.

25. Article 91-1 du décret du 20 octobre 2005 modifié visant les opérateurs de communication électronique et article 31 de la proposition de règlement européen sur la protection des données à caractère personnel dans sa version adoptée le 12 mars 2014 par le Parlement européen.

26. Formulaire de notification sur le site de la CNIL.

mission est habilitée à définir les formats et procédures applicables, au moyen d'actes d'exécution.

Frais de notification

L'adaptation des dispositifs de sécurité existant pour y intégrer un ou plusieurs modes de notification auprès d'autorités administratives représente des contraintes et des coûts pour les établissements financiers, notamment pour « *la mise en œuvre de systèmes qualifiés de détection* [27] ». Dans la LPM, il est clairement indiqué que « *les opérateurs sont tenus d'appliquer ces règles à leurs frais* ». De même, les frais engendrés par les contrôles sont à la charge des OIV[28].

Au-delà du coût de l'organisation et la mise en œuvre du dispositif de surveillance, en cas d'incident, chaque acte de notification va engendrer des coûts spécifiques. Le coût moyen engendré par la violation de données en France est estimé à 127 euros en moyenne par donnée[29] – soit, par exemple, pour 100 000 personnes concernées par une faille de sécurité, un total de 1 270 000 euros.

Dans un contexte réglementaire évolutif et en prévention face au développement de la cybercriminalité, le budget consacré à la sécurité de l'information est important. Il est à mettre en perspective avec les avantages apportés par la maîtrise des risques.

Même si la rédaction de la LPM ne donne pas d'indication sur le retour d'information dont les OIV peuvent bénéficier, les interactions constructives avec les régulateurs devraient représenter un avantage.

Sous-traitance et notification

Si l'entreprise a recours à la sous-traitance, elle reste pleinement responsable de la conformité de ses traitements aux règles applicables.

À ce titre, tout laisse penser que l'autorité compétente s'adressera à l'interlocuteur principal responsable des systèmes et données. Outre les prestataires en relation directe avec l'entreprise, il est important de contrôler toute la chaîne de sous-traitance, si les prestataires envisageaient à leur tour de confier une partie des prestations à un tiers.

Dans la LPM, l'article L. 1332-6-1 indique que les obligations s'appliquent aux OIV et « *aux opérateurs publics ou privés qui participent à ces systèmes* ». Ce point mériterait un développement lors de la rédaction du ou des décrets d'application.

Il est donc essentiel que les partenaires de l'entreprise fassent partie intégrante du processus de notification d'incident, afin de maîtriser l'exposition aux risques et de disposer le plus rapidement possible des informations nécessaires, pour répondre à l'obligation de notification. Il est primordial d'exprimer formellement aux partenaires potentiels non seulement le cadre réglementaire dans lequel ils s'inscriraient, mais également de préciser les modalités attendues pour respecter ce cadre. Il est important de préciser, dès l'expression de besoin et le cahier des charges, les critères de qualification d'un incident de sécurité et les modalités pratiques de notification.

L'encadrement contractuel peut contribuer à la sécurisation des échanges, dès lors qu'il est adapté à la prestation. Le contrat doit comprendre une ou plusieurs clauses rappelant les contraintes légales applicables et obligeant le sous-traitant à notifier à l'entité pour qui il travaille tout incident de sécurité. Il est envisageable de prévoir éventuellement des pénalités financières et une clause d'assurance spécifique. Les documents opérationnels devraient être intégrés au montage contractuel : plan d'assurance sécurité, plan de continuité d'activité et tests des procédures de notification, etc. Ces documents doivent intégrer les exigences techniques et permettre le contrôle, voire l'audit, du niveau de sécurité. La qualité de formalisation du contrat devra s'accompagner d'un suivi et d'un contrôle des prestations tout au long de son exécution.

La CNIL a prononcé un avertissement à l'encontre d'un prestataire de communications électroniques, suite à une violation de sécurité concernant plus d'un million de clients, et l'a publié le 25 août 2014[30]. Le prestataire avait bien rempli son obligation de notification auprès de la CNIL, mais cette dernière considère cependant que le prestataire a manqué à ses obligations d'assurer la confidentialité et la sécurité des données. La CNIL souligne que la société n'a pas fait réaliser d'audit de sécurité de l'application technique développée par l'un de ses prestataires et « *qu'aucune clause de sécurité et de confidentialité des données* n'était imposée » à ce prestataire. Dans ce cas, il s'agissait d'un sous-traitant secondaire au sous-traitant principal.

De plus, pour les établissements bancaires, quand les prestations externalisées sont qualifiées de services essentiels (ou PSEE)[31], ils devront conserver l'entière maîtrise des activités externalisées. Ils devront notamment encadrer contractuellement ces prestations, veiller à ce que le sous-traitant s'engage sur un niveau de qualité, mette en œuvre des mécanismes de secours et rende compte à l'établissement de manière régulière sur la manière dont est exercée l'activité externalisée.

Publication ou confidentialité ?

Même si l'objectif général des notifications de différentes natures est bien la consolidation de la sécurité globale, les modes de notification auprès de régulateurs différents entraîneront des effets différents : maintien de la confidentialité ou transparence. En cas de crise due à une faille de sécurité, la gestion de la communication devra s'adapter au cas par cas.

La LPM prévoit que les notifications effectuées auprès de l'ANSSI seront traitées de manière confidentielle[32].

Par ailleurs, cependant, dans le projet de règlement européen relatif aux données personnelles, l'autorité de régulation des données personnelles, comme la CNIL pour la France, peut imposer à l'entreprise qui a subi une faille de sécurité d'en informer les personnes concernées (clients, fournisseurs, etc.). La notification aux personnes leur permet de prendre des mesures afin de limiter les risques liés

27. Article L. 1332-6-1 du Code de la défense.
28. Article L. 1332-6-3 du Code de la défense.
29. « Cybersécurité : un vol de données coûte 2,86 millions d'euros en moyenne à une entreprise », *Les Échos*, 5 juillet 2013.
30. Délibération de la formation restreinte n° 2014-298 du 7 août 2014 prononçant un avertissement à l'encontre de la société Orange.
31. Arrêté du 3 novembre 2014, précité.
32. Article 22 de la loi de programmation militaire et L. 1332-6-5 du Code de la défense.

2. Exemple de clause relative à l'assurance « cyber »

(avec l'aimable autorisation de Gras Savoye)

« X souscrira, à ses frais, une police d'assurance couvrant tous les frais de X, y compris les dommages et intérêts qu'elle est obligée de verser à Y ou à un quelconque tiers, associés à toute Violation de sécurité (conformément à la définition visée ci-après) ou perte de Données personnelles, quelle qu'en soit la cause (y compris, de manière énonciative mais non limitative, une négligence ou une faute lourde de X et un acte illicite d'un tiers).

Cette police d'assurance couvrira, entre autres, les frais suivants :
(a) frais engagés pour aviser les personnes dont les Données personnelles ont été perdues ou compromises,
(b) frais engagés pour fournir des services de suivi de crédit (ou des services de protection de données analogues) et des services de rétablissement de crédit aux personnes dont les Données personnelles ont été perdues ou compromises,
(c) frais associés à des mises en cause au motif d'une Violation de sécurité ou d'une perte de Données personnelles, y compris les frais de litiges et de règlement, et
(d) frais d'enquête, d'exécution ou autres.

La couverture d'assurance sera plafonnée à 10 000 000 euros (dix millions d'euros).
Dans la présente Section, « Violation de sécurité » désigne
(1) toute situation au cours de laquelle X néglige de manipuler, gérer, stocker, détruire ou contrôler dûment ou divulgue sans autorisation
(a) des Données personnelles sous n'importe quel format ou
(b) des informations professionnelles tierces sous n'importe quel format spécifiquement qualifiées de confidentielles et protégées en vertu d'un contrat de confidentialité ou autre convention analogue,
(2) une violation accidentelle de la politique de confidentialité de X ou une appropriation accidentelle induisant une violation de toute loi ou réglementation applicable en matière de confidentialité des données ou
(3) tout(e) autre acte, erreur ou omission de X risquant raisonnablement de donner lieu à une divulgation non autorisée de Données personnelles (ou pouvant raisonnablement laisser croire qu'il y a eu divulgation non autorisée).

Cette assurance doit :
(a) nommer Y comme assuré additionnel au regard de l'intérêt assurable de Y,
(b) être de première ligne ou non contributive au regard des dommages ou frais assurés et
(c) être souscrite
(i) soit auprès d'assureurs domiciliés aux États-Unis et ayant une note d'au moins A- attribuée par A.M. Best et une note financière d'au moins 7,
(ii) soit auprès d'assureurs non américains ayant une note d'au moins BBB attribuée par Standard & Poor et
Sur demande de Y, X remettra à Y une ou plusieurs attestations d'assurance afin qu'il s'assure du respect des dispositions de la présente Section. »

à la défaillance. Cependant, la révélation de la faille devient largement publique et peut nuire à l'image commerciale de l'entreprise.

Application dans l'espace

En matière de sécurité des systèmes, la LPM s'applique naturellement au territoire français, sachant que les OIV sont responsables de leurs systèmes sans limitation de territoire. La coordination des différentes réglementations nationales applicables aux groupes bancaires internationaux reste un équilibre à trouver.

Le projet de directive SRI[33] a pour ambition d'harmoniser les politiques de sécurité de l'information au sein de l'espace européen.

En matière de sécurité des données personnelles, les projets européens intègrent la dimension transfrontière des transferts de données et visent à renforcer la coopération des agences administratives de protection des données, comme la CNIL et ses homologues.

Assurance

Depuis quelques années, les sociétés d'assurance ont développé des polices garantissant les dommages engendrés par les risques d'atteinte aux systèmes d'information, dits « cyber-risques ».

Ces contrats ont comme principales caractéristiques la prise en compte simple et rapide des garanties d'assurance en cas de cyberattaques et une réactivité des assureurs dans la gestion des sinistres, notamment en cas de notification d'incident de sécurité. Il s'agit de polices d'assurance dédiées aux cyber-risques, qui comprennent à la fois une couverture dommages, une couverture en responsabilité civile (RC) et des prestations d'assistance. Ces polices peuvent intervenir en complément des garanties existantes dans les programmes d'assurances classiques (RC, assurance contre la fraude, etc.).

Par exemple, ces polices peuvent proposer des garanties :
– en matière de RC: atteinte aux données confidentielles ou personnelles ;
– les frais d'enquêtes engagés par une autorité administrative et les sanctions administratives d'ordre pécuniaire ;
– les frais engagés en cas de gestion de crise : intervention d'un expert en sécurité informatique, conséquences d'une atteinte à la réputation, etc. ;
– les frais de surveillance et restauration des données, et ;
– les frais de notification.

Sur le marché français, une douzaine d'assureurs proposent des polices dites « cyber ». La plupart des produits cyber-risques assurent les frais de notification des incidents. L'un des avantages présenté par une police dédiée aux cyber-risques est qu'un éventuel sinistre serait déclaré et instruit auprès d'un seul interlocuteur, ce qui concourt à conserver la confidentialité. Un exemple de clause contraignant un prestataire à souscrire une police d'assurance figure dans l'Encadré 2.

33. Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union – 2013/048 (dite SRI).

Évolution des notifications

Les banques sont déjà soumises à un ensemble de dispositifs réglementaires visant à renforcer la sécurité de l'information. Face aux évolutions actuelles, elles doivent en permanence s'informer et préparer leur évolution. Cette adaptabilité et cette agilité représentent une nécessité pour assurer la protection optimale de leur système d'information et rester en conformité avec la réglementation.

Les décrets d'application[34] de la LPM sont parus le 27 mars 2015 et les arrêtés sectoriels sont en préparation.

Plusieurs projets européens visant à renforcer la sécurité des systèmes et des données sont annoncés. Dans l'attente de la formalisation des différents textes régulant les notifications d'incidents, il serait judicieux d'anticiper l'application des textes en projet. Des interrogations subsistent sur la manière dont les différents régulateurs vont coordonner leurs actions dans l'intérêt collectif.

Du côté des établissements financiers, la protection des systèmes d'information est un enjeu essentiel. Qu'ils soient OIV ou non, tous les établissements sont concernés par la notification des incidents de sécurité. Ils sont incités à construire ou optimiser les dispositifs de recensement des incidents et les modalités opérationnelles de leurs notifications auprès des différents régulateurs. ■

34. Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de confiance pour les besoins de la sécurité nationale. Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du Code de la défense.

RB e-LIBRAIRIE

Nouveauté

Au cours des deux décennies passées, le champ de l'innovation s'est élargi avec l'avènement sur la scène internationale de l'Asie, l'Inde y occupant une place de *leader*. Si le continent nord-américain est toujours un pôle puissant de R&D, il est dorénavant mis en partage avec d'autres pays qui renforcent la concurrence mondiale. L'Europe et la France en particulier, traditionnellement motrices, sont entrées dans cette compétition planétaire.
Le projet de novation, porté par un effort financier et un *management* performant, prend forme progressivement jusqu'à remporter un succès économique sur le marché pour devenir une innovation au sens plein. Comment innover, financer et mettre en œuvre un projet ? Ce livre expose point par point l'ingénierie d'un projet innovant et les relations avec les investisseurs. En reliant théorie économique, gestion financière, stratégie, *management* et *marketing*, il permet à tous les acteurs de se comprendre mutuellement pour collaborer efficacement à la naissance de nouvelles entreprises qui, espérons-le, deviendront des pépites.
Didactique et fondé sur l'expérience des auteurs, cet outil de pilotage et d'aide à la décision – le premier du genre – décrit :
– la place que doit prendre l'innovation dans l'économie générale et comment elle s'insère dans le fonctionnement des marchés ;
– la gestion de projet et l'incertitude, notions communes aux entreprises installées et aux *start-up* ;
– à partir de l'écriture du *Business Plan*, le montage et la dynamique d'évolution de l'entreprise d'innovation, les modèles de financement et les sources de revenus pour accélérer sa croissance ;
– la fiscalité et les aides publiques ;
– une méthode de valorisation de l'entreprise innovante.

MANAGEMENT & FINANCEMENT DE L'INNOVATION
Bernard Yon
et Bernard Attali
324 pages, 28 euros

Commandes, informations, catalogue :
revue-banque.fr
contact :
librairie@revue-banque.fr

RB REVUE-BANQUE.fr