Risques

Les cahiers de l'assurance

N° 101

Comité éditorial

Comité scientifique

Sommaire - n° 101 -

Éditorial

Notre précédent numéro était lié à cet évènement exceptionnel qu'a représenté la célébration du 100e numéro de notre revue. Il comprenait les contributions de 101 personnalités qui exprimaient leur perception du risque dans les années à venir. Il s'agissait d'un exercice très original de prospective explorant l'avenir dans un monde si évolutif et si marqué par l'émergence de nouvelles incertitudes, de nouveaux risques.

Le n° 101 se recentre au contraire sur l'actualité, mettant en lumière ce qu'elle contient de plus en rupture avec le passé, de plus surprenant et de plus incompréhensible dans les difficultés économiques et sociales que nous vivons aujourd'hui. C'est tour à tour la société française qui est interrogée, dans son impossibilité à retrouver une certaine harmonie de la société civile, telle que nous la décrit Yazid Sabeg. C'est ensuite ce nouveau péril inimaginable il y a quelques années encore, celui de cyberattaques ; et enfin ces domaines nouveaux et passionnants qui s'offrent à la gestion économique du risque, donc à l'assurance, à travers la situation économique incroyable que nous vivons.

Certes les politiques économiques tentent de s'accommoder de taux d'intérêt nuls, ce qui était impensable il y a encore peu. Ces trois sujets nécessitent d'abord et avant tout une compréhension d'un monde en train de naître. La plus grande gageure est de faire la part entre les faits réels et des visions plus fantasmatiques, liées à l'incompréhension, à la difficulté de l'analyse de faits et de phénomènes jusqu'alors inconnus. C'est d'ailleurs à cette confusion que s'attaque Luc Arrondel lorsqu'il s'interroge sur les rapports entre crise et peur du risque, et qu'à juste titre il souligne une corrélation qui détermine les comportements si prudents d'investissements de Français perturbés par les difficultés économiques actuelles. Mais la vie change et les comportements aussi. Nul ne nous dit que ce qui apparaît aujourd'hui comme peur, repli, fuite devant le risque, se poursuivra. On voit bien en ce début d'année 2015 que la montée des marchés boursiers contredit quelque peu cette vision, que nous avons tous, d'une aversion au risque renforcée en période de dépression.

Enfin, nous évoquons la cérémonie de remise du prix Risques. D'une certaine manière les deux ouvrages primés reflètent parfaitement la période actuelle. *L'affaire Snowden, comment les États-Unis espionnent le monde* est un fait politique d'une extrême gravité, parfaitement lié aux risques créés par la non maîtrise et l'absence de contrôle de la technologie. Mais, en même temps, nous avons souhaité nominer un autre travail, celui de Gérald Bronner – *La planète des hommes, réenchanter le risque* – qui dresse une analyse critique très solide du principe de précaution. Alors risques, peurs, gestion des nouveaux risques et prises à nouveau de risques, ainsi vont le monde et les sociétés. C'est ce dont nous avons essayé dans ce numéro de rendre compte.

Jean-Hervé Lorenzi

1.

L'espoir et la volonté

Yazid Sabeg

Président de Communication et systèmes (CS)
Ancien commissaire à la Diversité et à l'Égalité des chances

Yazid Sabeg

Président de Communication et systèmes (CS)
Ancien commissaire à la Diversité et à l'Égalité des chances

Entretien réalisé par Arnaud Chneiweiss, Jean-Hervé Lorenzi, Pierre-Charles Pradier et Daniel Zajdenweber.

Risques : Nous voudrions interroger trois hommes en un : le chef d'entreprise, l'ancien commissaire à la Diversité et à l'Égalité des chances et un homme qui a une vision forte du marché du travail.

Yazid Sabeg : C'est à l'issue d'une OPA que j'ai menée en 1991 sur la Compagnie des signaux, qui était une société active dans les domaines ferroviaire, de la défense et des télécommunications que j'en suis devenu le dirigeant. Je l'ai fait évoluer vers un modèle aujourd'hui *software* et *fabless* (1), dont la dénomination est aujourd'hui Communication et systèmes (CS). Altis, l'autre entreprise dont je suis le président, est spécialisée dans la conception et la fonderie de puces électroniques. CS est aujourd'hui complètement désengagée de la signalisation ferroviaire et s'est concentrée sur la conception et la réalisation de systèmes critiques au sens large, à forte composante sécuritaire, dans les domaines de la défense, de l'aéronautique, de l'espace, de l'énergie, surtout du nucléaire.

Risques : La problématique de la cybersécurité est-elle intégrée dans votre offre de systèmes ?

Yazid Sabeg : Complètement, même si CS fait beaucoup d'autres choses bien sûr. La cybersécurité irrigue toutes nos activités. Nous développons aussi bien des logiciels pour les systèmes d'information industriels ou militaires avec leurs infrastructures de communication sécuritaires que pour les moteurs d'avion. L'avionique ou le nucléaire nécessitent des logiciels très particuliers et à très haute sûreté. Dans ce cas, il s'agit de technologies de sécurité dites intrinsèques. C'est encore un autre niveau de cybersécurité : la sécurité forte pour des systèmes qui ne peuvent pas tomber en panne, ou, s'ils risquent de tomber en panne, ont une capacité de correction immédiate.

Altis, qui est indépendante de CS, est le seul fondeur français de semi-conducteurs, avec une capacité complète à fournir à toute l'industrie électronique des composants de souveraineté et des composants très sûrs. Elle va mettre sur le marché, d'ici un à deux mois, un chiffreur *hardware* de communications à très haut débit, voix, e-mails et SMS. C'est un processeur qui, par exemple, inséré dans votre smartphone, permettra de chiffrer et donc de protéger vos conversations téléphoniques. Il nous a fallu cinq ans pour le concevoir et le fabriquer intégralement en France. C'est une puce électronique et il va remplacer un équipement qui auparavant aurait pesé deux à trois kilos ! Nous avons développé un smartphone (Monolith) d'une toute nouvelle génération pour embarquer ce dispositif de chiffrement. Ainsi la NSA (2) ou d'autres pourront toujours essayer d'intercepter les communications mais ils ne pourront pas disposer des contenus chiffrés sauf à mobiliser des moyens colossaux. Le développement de ce produit unique représente plusieurs années de travail pour une trentaine de personnes.

Risques : Chiffrage, protection des données. Quelle est votre position sur ces questions, à titre personnel et en tant que chef d'entreprise ?

Yazid Sabeg : Le droit de protéger les informations à caractère personnel ou les secrets d'une entreprise fait partie des libertés individuelles et fondamentales. Pour le chef d'entreprise, il y a deux enjeux majeurs en matière de cybersécurité : l'intrusion, qui peut compromettre le secret des projets de développement (l'espionnage industriel), et le sabotage par des intrusions

malveillantes. Outre nos produits de chiffrement, nous avons développé deux autres types de produits : des services Web certifiés – signature électronique, authentification, non répudiation, archives à valeur probante – qui viennent d'être homologués par l'Agence nationale de la sécurité des systèmes d'information (Anssi) ; et un produit appelé Siem (Security information and event management) qui analyse ce qui se passe sur le réseau en temps réel pour détecter les intrusions et les fraudes. Par exemple, un intrus qui tente de forcer un réseau ne peut le faire qu'en testant des milliers et des milliers de codes d'accès. Siem permet de détecter ce comportement immédiatement. Ce sujet préoccupant a conduit l'Anssi à mettre en place des règles et des exigences de sécurité renforcées pour les infrastructures stratégiques ou vulnérables – électricité, gaz, télécommunications – très exposées aux attaques. Mais il faut souligner que la France est malheureusement très en retard dans ce domaine par rapport à d'autres pays européens, principalement par manque de stratégie nationale volontariste. Les risques sont peu analysés ; la planification de la réponse au risque manque de méthode et elle prend beaucoup de temps. Enfin, on continue à acheter des produits américains, israéliens ou britanniques, bien qu'ils ne soient pas sûrs car ils sont compromis.

Risques : Passons maintenant à un sujet dans lequel vous vous êtes beaucoup investi : la politique d'intégration. Quel regard portez-vous sur les politiques mises en œuvre ces trente dernières années ?

Yazid Sabeg : Je pense que depuis des décennies la France n'a pas su et ne sait toujours pas gérer sa diversité, et qu'elle est même en train de régresser. Les problèmes centraux sont économiques et sociaux. La question de la compatibilité culturelle ou religieuse des migrants ou de leurs enfants qui sont français, ou la menace qu'elle constituerait pour l'identité sont des sujets certes sensibles mais périphériques et devenus incontournables parce qu'essentialisés pour des raisons politiques.

Une des questions de fond est de savoir de quoi est constituée la population de la France du XXIe siècle ? Il faut étudier de manière objective cette question et faire preuve de lucidité. Je suis un farouche partisan du comptage. Il est essentiel parce que les chiffres permettent précisément d'être objectif. La France est peuplée de Caucasiens, d'Arabo-Berbères, de Noirs, d'Afro-Américains qui sont des Français à égalité de droits et de devoirs. Il faut le dire et l'expliquer aux enfants dès la maternelle. C'est tabou à tel point qu'un enfant de dix ans est capable de dire à son camarade « retourne dans ton pays », quand vous n'êtes pas un « bon Blanc ». Ce qui m'est arrivé, ce qui est arrivé à mes enfants. Il est essentiel de traiter de la diversité de la population de la France et de sa diversité religieuse. Ce pays est peuplé de catholiques, de protestants, de juifs et de musulmans, qui ont le droit de l'être – articles II, IV et XII de la Constitution. Et ils ont le droit de l'être comme ils le veulent, voilés s'ils le veulent. Avec une croix, une kippa, des babouches, avec ce qu'ils veulent. C'est leur droit, c'est un droit fondamental.

L'identité de la France n'est nullement menacée par la diversité mais par le fait que c'est un pays en ruine économique et sociale où la conscience civique a disparu. La France est une nation forte qui s'est pourtant construite sur l'oubli des origines de ses citoyens. Cet oubli est le fondement même de l'assimilation républicaine qui elle-même est incompatible avec le communautarisme ou le multiculturalisme. C'est une première observation. Ensuite il faut regarder comment les uns sont traités par rapport aux autres. Je pense que les discriminations ont des conséquences sociales et économiques spécifiques. Les Français discriminés ne sont pas seulement des pauvres, ils sont, en plus d'être discriminés, relégués territorialement et ne bénéficient pas de la mobilité sociale – ce fameux ascenseur qui est depuis bien longtemps en panne. La République, la laïcité, etc. sont hélas devenues des concepts totalement inopérants car les inégalités qui résultent des discriminations ont eu raison de notre cohésion nationale.

Je suis un républicain au sens littéral du terme. J'ai bénéficié d'une éducation républicaine bien que fondée sur l'oubli de mes origines. C'est ça, la République. Pour moi, mon arrivée en France est une

page blanche. Ce qui pourtant n'est pas tout à fait vrai. Vous voyez, à l'école j'ai appris « nos ancêtres les Gaulois », ce qui est faux, mais j'ai intégré cette vérité organique.

Deuxième point important : quels sont les résultats de la politique de peuplement de nos territoires ? En termes de diversité sociale – et, disons-le, ethnique ou socio-ethnique –, c'est un échec complet. On a spécialisé les quartiers. C'est une monstrueuse erreur. On a essayé de corriger en améliorant la qualité du logement – et on l'a assez bien fait dans plus de la moitié des quartiers défavorisés en France –, mais l'État, sous la pression budgétaire, s'est aujourd'hui désengagé de cette politique publique et n'investit plus sur ces quartiers et leurs populations pas plus qu'il ne corrige les inégalités qui s'aggravent. Il n'y aurait plus d'argent, alors même que rien ne saurait justifier l'inégalité d'accès au logement, à l'emploi ou à l'éducation ? J'ajoute que l'Éducation nationale en tant qu'institution ne fait pas son travail en matière d'ouverture ou de promotion sociale. Il y a donc toujours des problèmes extrêmement lourds dans les quartiers. Il faudrait des méthodes différentes, organiser différemment la carte scolaire prioritaire. Comment pouvez-vous justifier qu'il n'y ait qu'un ou deux lycées généraux en Seine-Saint-Denis – alors que ce département compte un tiers des élèves à scolariser en enseignement secondaire –, et qu'il y en ait 45 ou 50 à Paris ? C'est un réel problème et ce n'est pas uniquement en introduisant la morale laïque que la donne va changer. Notre système éducatif est à bout et socialement totalement déséquilibré.

Risques : L'une des idées de la Révolution française était qu'en faisant disparaître les inégalités de savoir on ferait disparaître les inégalités sociales. Mais savons-nous donner un véritable accès à l'éducation ?

Yazid Sabeg : La mobilité sociale est déterminée par l'ascension sociale, le désir d'ascension sociale. L'égalité des chances (*Equal opportunity* au sens anglo-saxon du terme), c'est donner la même boîte à outils à chacun. Je suis convaincu que cette croyance est limitative. Si je donne la même boîte à outils à Mohammed qui habite à La Courneuve, et à François qui habite le XVIe arrondissement, ils ne bénéficieront pas d'opportunités équivalentes parce que le père du premier est ouvrier et que le père du second est enseignant. La mobilité sociale est le fondement de tout. Je suis fils d'agriculteur, fils d'instituteur, fils de professeur, fils d'ingénieur, et je deviens moi-même ingénieur au bout de deux ou cinq générations, selon le statut social de mes parents. C'est le modèle social des XIXe et XXe siècles ; qui a fonctionné, mais qui ne fonctionne plus tant le déterminisme social est fort dans notre pays.

Avec la massification de l'enseignement supérieur, le diplôme comme moyen d'intégration sociale, d'ascension sociale, n'est même plus suffisant. Le nombre de jeunes diplômés chômeurs enfants de migrants est colossal. Il y en aurait 250 000. Ils ont eu accès à certaines filières du système éducatif, ils ont eu un diplôme, mais ils n'ont pas de travail.

L'expérience d'ouverture sociale et de diversification du recrutement de Sciences Po va dans le bon sens. Elle est réussie et démontre que cela peut fonctionner, mais c'est une initiative qui reste quasi unique. J'avais dit à Jack Lang et Richard Descoings : « Il faut qu'une grande école bouge. Allez chercher les meilleurs élèves là où ils sont. Mais forcez-vous à aller les chercher – je n'ai pas employé le mot de « quota » mais de « quotité » – dans les quartiers ». Il y a forcément des élèves qui valent ceux des centres villes, qui eux sont favorisés et à qui on parle de Sciences Po depuis qu'ils sont nés. Allez les chercher. Ils l'ont fait avec audace et ça a marché. J'aurais voulu que l'École polytechnique le fasse également… Quand j'étais en fonction, je voulais qu'il y ait 30 % de boursiers, au titre de l'ouverture sociale, dans les classes préparatoires et les grandes écoles. Que n'ai-je entendu !

Risques : D'autres pays ont réussi à s'en sortir. Comment ont-ils fait ?

Yazid Sabeg : Les Américains ont créé l'Affirmative action, c'est-à-dire l'équité. Ce n'est pas seulement l'égalité de traitement mais la volonté de corriger les inégalités en agissant au-delà du droit commun. Ils ont constaté qu'il n'y a rien de plus injuste que de

traiter de façon égale des situations inégales. Ils ont débattu des vrais problèmes démocratiquement et mis en œuvre des politiques correctrices fondées non pas sur l'égalité mais sur la justice.

Le président de la République ne parle aujourd'hui que de République et de laïcité alors que ce n'est pas le sujet du moment. Le plus important pour réussir à bâtir une société, c'est que tout le monde sente qu'il appartient à la société française. Gambetta a dit que la vraie démocratie ce n'est pas de reconnaître des égaux mais d'en faire ! Pour y parvenir, il faut notamment que chaque citoyen soit fier de son pays, il faut une fierté d'appartenance nationale. Or, on ne peut pas être fier de son pays si votre pays n'est pas fier de vous. On ne peut pas être fier de son pays si vous n'êtes pas fier de votre père. Tant que notre société traitera en effet ses populations de migrants par l'exclusion et le déni pour les délégitimer, sans reconnaître leurs apports à l'édification de notre pays et à notre sens commun (ce qui nous est commun) nous n'arriverons à rien.

Risques : Vous venez d'introduire la transition sur le troisième sujet, la reconnaissance de la force de travail et la reconnaissance du besoin de travail. Le fait que cette aggravation du malaise se fasse sur un fond de chômage croissant, ce n'est pas une coïncidence ?

Yazid Sabeg : Bien sûr que non, la valeur et la place du travail sont des composantes de la crise d'aujourd'hui. Ce n'est pas spécifique à la France mais la France est un pays où les privilèges subsistent et sont puissants. On a parlé du système éducatif, on pourrait parler de toute autre chose. Il y a deux ou trois sociétés françaises. D'abord une société blanche et une société colorée, qui n'ont pas les mêmes caractéristiques, ni les mêmes attributs, ni le même avenir, ni les mêmes perspectives. Il faut aussi reconnaître qu'il y a plus de chômage chez les migrants et leurs enfants. Ils sont dix millions de personnes, c'est un chiffre colossal. Ensuite, vous avez les protégés et les moins protégés, les nantis et les moins nantis, c'est-à-dire les gens qui ont une parcelle de pouvoir, une parcelle d'autorité. Et puis vous avez des catégories sociales extrêmement dures à démanteler : les castes. Elles subsistent et prospèrent largement en France.

Risques : Le prix Risques en 2013 a été décerné à Laurent Davezies pour *La crise qui vient*, qui porte sur la désindustrialisation profonde de la France. Mais a-t-on aujourd'hui envie d'être ouvrier ?

Yazid Sabeg : La France a effectivement perdu sa compétitivité, et le plus grave, sa capacité d'innovation est concurrencée et menacée. C'est un processus qui va de pair avec la désindustrialisation et la baisse de rentabilité de l'industrie, c'est un processus important qui sera difficile à enrayer. Par exemple notre groupe dispose en France de la plus grande usine d'Europe de semi-conducteurs, Altis. L'activité est robotisée à 80 %. Nous allons réaliser un chiffre d'affaires croissant avec une quasi-stabilité de notre effectif de collaborateurs directement impliqués dans la production. C'est inhérent à notre industrie. Toutefois toute activité industrielle induit de nombreux emplois de services sans lesquels toute production industrielle serait impossible. Je crois effectivement que la notion d'ouvrier a elle-même profondément changé. Dans une raffinerie, il n'y a plus personne qui circule dans des allées polluées, tout est automatisé. Dans les centrales nucléaires non plus. Je pense que de ce point de vue beaucoup de choses restent à faire dans le domaine des industries à coûts décroissants et à rendements croissants. Il y a encore beaucoup de choses à faire, notamment dans les domaines de la chimie, de la pharmacie, des biotechnologies, de l'électronique et de l'automobile.

Mais il manque une volonté politique pour créer les conditions d'une reprise de l'investissement et du renouveau industriel de notre pays.

Les industriels s'en vont, ils n'investissent plus en France mais à l'étranger. On se demande pourtant encore pourquoi les entreprises se portent mal. Les grands ne sont plus là. Le CAC 40 réalise 80 % à 90 % de son activité hors de France. C'est grave.

Risques : Peut-on dire un mot sur l'Europe d'un point de vue économique ? Les jeunes Européens qui ont envie d'entreprendre vont aux États-Unis, parce qu'ils y trouvent deux choses : un vrai marché unique, et le moyen de faire prospérer une entreprise.

Yazid Sabeg : Il y a bien un marché unique en Europe – les produits circulent librement d'un pays à l'autre – mais nous n'avons que peu de géants européens. Il y a encore des habitudes nationales, des domaines exclusifs. Il y a des freins institutionnels à la concentration. Mais le marché américain a mis des décennies à se constituer, il ne faut pas l'oublier non plus. Aujourd'hui dans les secteurs de pointe – les start-up – le marché européen est insuffisamment ouvert. L'information ne circule pas et il n'y a pas de préférence européenne. Cela prendra du temps, mais il est essentiel d'y parvenir.

Risques : Pour conclure, comment voyez-vous la France dans les années qui viennent ?

Yazid Sabeg : Le problème central c'est de rétablir une société cohérente, de confiance et de responsabilité dont les citoyens partagent des aspirations communes, un destin commun. Le philosophe situationniste Raoul Vaneigem disait : « Seule nous est commune l'illusion d'être ensemble ». Il s'agit d'inverser ce triste constat. Nous sommes dans une situation telle que la première des choses est de redonner du sens et de la cohésion à notre société qui est profondément troublée et déstabilisée. Pour y parvenir, il faut que les hommes politiques, qu'un homme politique s'en rende compte et agisse. C'est possible car notre pays est relativement réactif et prêt à accepter les efforts nécessaires. Les castes, les privilèges… il faudra remettre en cause beaucoup de choses profondément enracinées dans notre culture, dans notre « identité » comme on dit aujourd'hui.

Notes

1. Une société fabless *de semi-conducteurs est spécialisée dans la conception et la vente de puces électroniques. Par contre, la fabrication des puces elles-mêmes est sous-traitée à des sociétés spécialisées de fabrication de semi-conducteurs.* Wikipédia.

2. NSA : National Security Agency ou agence nationale de la sécurité des États-Unis.

2.

Cybersécurité *terra incognita*

INTRODUCTION

Charlotte Dennery

Il y a seulement un siècle, qui aurait évoqué le risque nucléaire dans la presse ? Personne ! Il y a seulement dix ans, qui aurait parlé de cyber-risques dans la presse ? Personne non plus !

C'est le propre des risques liés aux nouvelles technologies que d'être au début un sujet d'experts, de spécialistes, voire un sujet de science-fiction. Et puis, après quelques attaques, la science-fiction devient réalité, avec tous les effets dramatiques auxquels nul n'avait même osé songer. Alors, le sujet devient largement médiatisé. À cet égard, il est impressionnant de voir le nombre de livres, d'articles, de cahiers qui ont été écrits sur le cyber-risque au cours du dernier trimestre.

Mais que peut-on dire précisément aujourd'hui de ce risque ? Comment peut-on caractériser les cyberattaques ? Qui en sont les principales victimes ? Quels sont les motifs de ces attaques ? Peut-on mettre en place des méthodes de prévention ? Quelles sont enfin les couvertures assurancielles possibles et y-a-t-il un marché de la réassurance ?

Les types d'attaques sont extrêmement variés et leur criticité n'est pas toujours mesurable immédiatement, mais force est de constater qu'elles sont devenues de plus en plus sophistiquées. Elles vont du déni de service au piratage de données clients, en passant par le *phishing* (1) d'information sur les collaborateurs, la divulgation de données sensibles de l'entreprise, le blocage des systèmes d'information ou l'inoculation de malware (2). Leurs conséquences peuvent être immédiatement détectées ou à l'inverse ne surgir que plusieurs mois après l'attaque, mais il n'est pas rare qu'elles soient graves. ***Anne Souvira*** nous en donne un aperçu édifiant dans son article.

Abordons maintenant les ressorts qui poussent un agresseur à lancer une attaque. Les mobiles peuvent tout d'abord être d'ordre politique : il s'agit d'attenter à la réputation d'un acteur que l'on souhaite voir décrédibilisé ou affaibli. Le hacker ***The SnowCrew*** se présente ainsi comme un nouvel acteur du jeu politique, un redresseur de torts comme pouvait l'être Robin des Bois à une époque, un acteur de la transparence cherchant à améliorer le fonctionnement de notre démocratie et à dénoncer les errements d'un ou de plusieurs États. Mais les attaques ont – dans leur grande majorité – des visées économiques et financières : espionnage de la concurrence, appât du gain, demande de rançon, revente de données personnelles sur un marché noir, mise à l'arrêt temporaire des capacités de travail d'un concurrent. Enfin, ils peuvent prendre une dimension géostratégique comme l'ont révélé les affaires WikiLeaks ou Snowden.

Tous les auteurs de ce cahier se rejoignent pour considérer que la meilleure des protections contre ce risque réside dans la sensibilisation et la formation des acteurs ainsi que dans les changements de comportements. Prendre en compte la problématique du cyber-risque doit se faire, selon ***Jean-Paul Mazoyer***, à tous les niveaux de l'entreprise et nécessite une impulsion de la direction générale. La logique sécuritaire doit irriguer l'ensemble de l'organisation et doit être considérée comme vitale par tous les collaborateurs.

De manière plus systématique, la culture de la méfiance doit prévaloir. Bien sûr, la sensibilisation ne suffit pas et des outils technologiques ont été développés pour accompagner les entreprises dans la réduction de leurs vulnérabilités. ***Alain Bénichou*** et ***Agnieszka Bruyère*** présentent dans leur article une liste exhaustive des solutions informatiques proposées par IBM à ses clients en matière de protection, détection ou gestion des incidents de sécurité informatique.

Xavier de Marnhac et ***Yves Mathian*** insistent quant à eux sur la nécessité pour la France de garder une souveraineté en matière de suivi des cyber-risques et de méthodes de protection. Ils considèrent que sur le plan institutionnel, la France s'est mobilisée à temps pour imposer aux acteurs les plus sensibles (OIV : opérateurs d'importance vitale) des normes strictes en matière de sécurité des systèmes d'information. Ils déplorent toutefois qu'en l'absence de politique industrielle de soutien au marché de la protection informatique et du cryptage, la France se retrouve aujourd'hui dans une situation de dépendance vis-à-vis d'acteurs américains, israéliens, chinois ou indiens. En tout état de cause, quelles que soient les mesures de protection mises en œuvre – juridiques, technologiques, comportementales – rien ne remplacera la définition et la mise en œuvre par les entreprises ou les organisations d'une cyber-stratégie globale qui sorte de l'approche en silo, comme en témoigne ***Frédérick Douzet***.

Le marché de l'assurance des cyber-risques s'est développé aux États-Unis dans les années 2000 et est en forte croissance. Vu la multiplicité des risques à couvrir, la cyberassurance combine en général des garanties dommages et des garanties responsabilité civile. ***Clotilde Zucchi*** nous donne un aperçu du contenu et de la disparité des contrats qui peuvent être souscrits en matière de cyberprotection. Ce marché représente en Europe moins de 500 millions d'euros tandis que le marché aux États-Unis représente plus de deux milliards de dollars américains. Ces risques sont toutefois difficiles à tarifer en raison du manque de données historiques sur les sinistres et sur leur coût effectif pour l'entreprise. Enfin, jusqu'à récemment, la taille des portefeuilles et la demande des assureurs ne justifiaient pas un appel à la réassurance. Mais de plus en plus, la gestion des cumuls de risques nécessiterait une expertise propre et une modélisation adaptée. Cette expertise est encore embryonnaire et peu mature comme le précise ***Didier Parsoire***.

Dernière évidence qui transparaît en filigrane dans chacun des articles : nos entreprises manquent cruellement d'expertise et de compétence en matière de cyberprotection et la problématique est mal appréhendée par les dirigeants. Faisons un pari : les choses changeront quand la génération Z, qui a été élevée dès son plus jeune âge au contact d'Internet et des médias sociaux, se verra chargée de postes de responsabilités.

Notes

1. Phishing *: « hameçonnage ».*

2. Malware *: « logiciel malveillant ».*

Regard d'une spécialiste de la lutte contre la cybercriminalité

Anne Souvira

Commissaire divisionnaire, chef de la brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti)

La cybersécurité est un devoir pour protéger les données, le patrimoine et la réputation. Celle de tous dépend de celle de chacun et inversement. La devise des mousquetaires n'a jamais été autant d'actualité. Face au hacking, à ses moyens et à ses conséquences patrimoniales, seule la cybersécurité « d'un pour tous et de tous pour un » pourra contenir ou mettre en échec les attaquants.

Le patrimoine menacé

On n'a jamais autant parlé, à la fin de 2014 [Robert, 2014] et au début de 2015, de cybermenaces (1) et de leur corollaire, la cybersécurité, qui paraît la réponse la plus adaptée pour les contenir. Inhérentes au développement d'Internet du fait de l'usage accru de technologies en constante évolution, ces cybermenaces sont la rançon d'une révolution numérique [Souvira, 2014] dont les prémices furent annoncées dès 1977 dans le rapport Nora-Minc [Minc et Nora, 1978], qui ne pouvait entrevoir la part d'ombre de l'informatisation. Ainsi, particuliers, administrations et organisations font face au sabotage de leurs systèmes d'information (SI), à l'espionnage de concurrents ou d'États et aux atteintes à leur réputation à travers les réseaux sociaux, dont les mobiles sont le cyber-hacktivisme contestataire, la malveillance, l'appât du gain par appropriation du patrimoine informationnel, l'économie en recherche et développement ou la revente des données personnelles sur les marchés noirs. L'attaque, aux conséquences toujours graves (chômage, suicide, disparition d'entreprise, coût, etc.), est fonction de la taille et du secteur d'activité de la structure, ainsi que de la fréquentation du site Internet de celle-ci. Le responsable des systèmes de traitement automatisé de données (Stad) doit s'en prémunir.

Or, si depuis longtemps on alerte les organisations, et que les Livres blancs de 2008 et de 2013 sur la défense et la sécurité nationale ont permis des avancées, sur le terrain, on peine à discerner des progrès tangibles en matière de cybersécurité (2). Cette carence facilite l'attaque et constitue un danger aussi financier que juridique. Est-il possible et souhaitable de s'assurer contre ces risques, et quelle forme revêtirait l'expertise

pour en déterminer la prime ? N'empêcherait-on pas le maître du système de prendre conscience de l'impérieuse nécessité de la cybersécurité ? Les réponses se mesureront à l'aune de la jurisprudence et de la structuration d'une filière d'assurance entre obligations légales, état de l'art et nécessités commerciales. Cela pourrait être de nature à élever le niveau de cybersécurité.

Les différents modes d'attaque

« Ils ne mouraient pas tous, mais tous étaient frappés » (La Fontaine). Les menaces ne sont pas virtuelles, et les données se trouvent toujours quelque part dans un *data center*, où les hackers les dérobent pour en tirer profit. La réussite de l'attaque dépend du niveau de cybersécurité.

Le risque zéro n'existe pas. Les organisations, vu le niveau variable de leur cybersécurité, succombent aux attaques des e-criminels, quand le sujet est pourtant débattu dans bien des cercles. Du faux technicien informatique au *malware* CryptoLocker, les dossiers de la Befti montrent un manque de politique de sécurité ou une naïveté coupable. Les rapports des éditeurs de logiciels (3) confortent cette vision, et l'Europe mesure la nécessité d'instaurer un niveau commun de cybersécurité pour ne pas fragiliser l'ensemble.

Les modes opératoires illustrent l'importance de la politique de cybersécurité sans laquelle réussira telle campagne de *phishing* (4) ou d'infection virale contractée sur un site, « point d'eau » très fréquenté infecté à dessein (5).

Extorsion de fonds

Les auteurs scannent les vulnérabilités du SI, exfiltrent les données personnelles des clients, prospects ou salariés, et exigent une rançon en bitcoins (6) pour ne pas les divulguer. Le refus entraîne leur révélation sur des sites de partage de contenus (7) et une atteinte à la e-réputation. Le SI non sécurisé constitue un risque élevé financièrement et pénalement.

Les données rançonnées sont rendues inaccessibles, car la victime introduit le code malveillant, le « rançongiciel », dans le poste de travail, tel CryptoLocker, qui chiffre les données et les fichiers accessibles en écriture. Pour recouvrer les données, une boîte de dialogue invite à suivre les indications figurant dans des fichiers non chiffrés, contre une rançon en bitcoins. Des liens sont fournis pour se les procurer et procéder au déchiffrement des données grâce à la clé reçue en échange. Dans les organisations à faible cybersécurité, l'ouverture sans vigilance d'une pièce jointe infectée n'est pas détectée par l'antivirus, rarement mis à jour. Sans sauvegarde sécurisée en dehors du SI, il sera rarement possible de récupérer ses contenus.

Défiguration de site ou fausse page

La défiguration de site ou la fausse page entravant l'activité résultent du défaut de mise à jour de l'outil de gestion de contenu des sites Internet.

Attaque par déni de service

Le déni de service distribué (DDoS (8)) par des activistes, des concurrents, l'exfiltration de données résultant de la prise de contrôle d'un poste de travail puis du SI, sur l'appel d'un faux technicien informatique, peuvent aussi bien cacher des menaces avancées (APT (9)). La victime peut servir de rebond à l'attaquant, qui vise en fait un tiers, peut-être du secteur des opérateurs d'importance vitale (OIV).

Contrefaçon de DCP

La contrefaçon (10) de bases de données à caractère personnel (DCP) est réalisée par injection de code malveillant et permet la collecte des DCP, faute de sécurisation du système de traitement prévu et réprimé

fortement par le Code pénal (11), soulignant les obligations des opérateurs de communications électroniques (OCE) et des OIV.

Interception de code à usage unique

En sus des *malwares* bancaires, l'interception de code à usage unique pour authentifier un achat est le signe de la présence d'un virus dans le smartphone.

Faux ordre de virement

Ils touchent les particuliers et les organisations de toutes tailles, par l'ingénierie sociale (12), une baisse de vigilance contournant les dispositifs de contrôle interne.

Utilisation frauduleuse de lignes téléphoniques

Des escroqueries ont également lieu par l'utilisation frauduleuse des lignes téléphoniques de l'autocommutateur (13) après la prise en main de la ligne de télégestion ou d'une messagerie vocale, ou encore par l'utilisation du compte de l'organisation en l'absence de mise à jour et de contrôle des fonctionnalités (appels vers des GSM étrangers, numéros surtaxés, sites pornographiques, sites de voyance ou de jeux à instant gagnant).

Quelle politique de sécurité ?

Il y a un réel danger de remise en question de la confiance dans l'économie numérique, l'industrialisation des attaques et la vitesse de leur propagation permettant aux e-criminels de s'enrichir.

C'est pourquoi la stratégie de l'Union européenne (UE) vise à « prévenir les perturbations et les attaques des systèmes de télécommunications européens et à y apporter une réponse. (14) » L'UE définit le risque comme toute circonstance ou tout événement ayant une incidence négative potentielle sur la sécurité. On vient de le montrer, l'absence d'une politique de sécurité des SI ou de mise en œuvre de celle-ci a une incidence négative sur la sécurité des données, les affaires et même la souveraineté.

Sensibiliser et éduquer les internautes

Parallèlement, il s'est imposé que la protection de l'internaute était au cœur de la lutte contre la cybercriminalité lors des travaux menés sous l'égide du procureur général Marc Robert, dont l'objectif était de permettre d'élaborer une stratégie globale pour lutter contre celle-ci. Il convenait de prendre la mesure du danger que constituait l'internaute – perçu en tant que maillon faible, assis entre la chaise et le clavier, dans sa sphère personnelle et professionnelle – pour lui-même et pour autrui, et de l'en protéger. Des préconisations (15) ont donc été apportées pour adapter le droit pénal ou processuel, mais surtout pour développer la prévention des risques par la sensibilisation et l'éducation des internautes. Car il ne sert à rien d'élever des défenses en château fort, si d'un clic on abaisse le pont-levis…

Connaître les dangers grâce à une culture de la cybersécurité est un prérequis pour rendre la tâche plus difficile aux hackers et rentabiliser des investissements techniques coûteux mais indispensables pour protéger nos données personnelles – « or noir » du siècle – de leur convoitise.

On légifère pour protéger le consommateur de constantes évolutions technologiques tout en voulant exploiter ses données. Il faut, dans ce domaine peu consensuel, concilier business, droit à la vie privée et à l'oubli, et réclamer aux forces de l'ordre l'identification de hackers à l'étranger, dans le respect de l'équilibre entre sécurité publique et intimité de la vie privée, bien étalée par ailleurs ! On se méfie des GAFA (16) tout en utilisant des comptes Google, Gmail, iTunes ; on achète sur Amazon et on se livre sur Facebook et Twitter. Pour Candy Crush, toutes nos données sont accessibles en entrée libre via le Patriot Act (17).

La sécurité « intégrée »

Mais a-t-on porté attention à la troisième édition du Mois européen de la cybersécurité en octobre 2014, si peu relayée par les médias classiques ?

Elle est restée cantonnée au cybermonde et ses articles des magazines spécialisés poussés au gré des nombreuses manifestations consacrées aux DSI, RSSI, CIL (18), ou à l'occasion de colloques (19) diffusant la réflexion des informaticiens, des experts juristes ou des praticiens du droit. De même sont restées entre soi les parutions des éditeurs de logiciel faisant état de prévisions communes sur le risque que constituent la mobilité, en tant qu'appareils connectés « métro, boulot, dodo », les objets connectés domotiques et médicaux, et le danger des comportements encore immatures des personnes et des organisations.

La rencontre de ces comportements et des hautes technologies qui dépassent notre entendement de futur « homme augmenté » commande aujourd'hui non plus seulement de sensibiliser mais de passer à l'action et de prendre des mesures de sécurité « *by design* » (20) pour tous : développeurs, écoliers, lycéens, universitaires, etc. Car nul n'échappera à ces technologies qui facilitent ou qui gâtent la vie.

La cybersécurité telle une seconde nature permettra de contenir le cybercrime s'attaquant à l'État, aux organisations et aux particuliers. Chacun, par sa cyberattitude, peut et doit contribuer à en réduire le coût (21). C'est une nécessité, vu l'inégalité des armes, des moyens juridiques et financiers au profit des hackers dans la lutte contre les cybermenaces.

Du niveau de cybersécurité de chacun dépend la cybersécurité de tous, et plus généralement la cyberdéfense de la France (22).

Une industrie à développer

Il est indispensable de connaître le risque numérique pour mieux le maîtriser et développer des capacités en cybersécurité pour la souveraineté nationale. Aussi, dans la réflexion gouvernementale sur la nouvelle France industrielle (23), présentée fin 2013, le plan 33 concerne la cybersécurité (24). Sont prévus tant des actions préventives auprès des personnes que le développement d'une industrie de cybersécurité de confiance (25) pour les produits « solutions de sécurité ». Sous l'égide notamment de la délégation ministérielle aux industries de sécurité, créée en novembre 2014 (26), les structures de toutes tailles monteront en compétence par la qualité des processus de sécurité et leur intégration dans les SI, par la surveillance 24 heures sur 24 des incidents et la rapidité des réponses apportées en liaison avec les centres de veille, d'alerte et de réponse aux attaques informatiques (CERT (27)).

Entre sécurité publique et libertés individuelles

La lutte contre la cybercriminalité qui attaque le patrimoine de la nation via les particuliers ou les organisations est une lutte inégale où la prévention reste l'arme la plus efficace.

Malgré l'arsenal pénal de lois (28) adapté, bien qu'éparpillé dans plusieurs codes (29), et la gravité des conséquences des faits, les textes restent sous-utilisés. Le droit processuel évoqué dans le rapport sur la cybercriminalité [Robert, 2014] est encore inadapté au Deep Web, où les informations ne sont pas indexées. Il en est de même des forums fermés du Darknet, où se déroulent les conversations inaccessibles des bandes organisées d'e-criminels, qui échappent ainsi à la justice.

Les moyens des forces de l'ordre dépendent de l'équilibre requis par la Convention européenne des droits de l'homme (CEDH) entre les exigences de la sécurité publique et celles relatives à la préservation des libertés individuelles, à concilier toutefois avec l'exploitation des données personnelles des consommateurs pour développer l'activité des entreprises. « Dans le cadre de l'examen de la proposition de règlement européen sur la protection des données,

l'IAB France et le SRI soutiennent une solution respectueuse des intérêts des internautes tout en préservant le potentiel de croissance de l'économie numérique [30]. »

Le projet de loi numérique de la secrétaire d'État Axelle Lemaire, qui prévoit de recourir aux nouvelles forces numériques créatives, devra prendre la mesure des cybermenaces pesant sur l'économie, la massification des fraudes et leur vitesse d'exécution ne plaidant pas pour la confiance dans l'économie numérique, ce dont elle a justement le plus besoin. L'installation d'un sentiment de « cyberinsécurité » pourrait entraîner une désorganisation du marché du numérique due à une fracture entre des particuliers ou petites structures se mettant en retrait de l'économie numérique et d'autres qui pourraient jouer le tout-numérique.

Le contexte stratégique européen et français, industriel et commercial de sécurité des SI et des données qui y transitent transparaît dans les plaintes toujours croissantes. Aussi, les services participent, par les enquêtes et la sensibilisation, à la promotion de la cybersécurité. Ils rendent visible l'action de l'État contre la cybercriminalité influant sur le sentiment de cybersécurité. La meilleure défense contre les cyberprédateurs est d'élever le niveau de cybersécurité. Celui-ci réduit le risque de succomber aux cybermenaces, pas toujours assurables pour l'organisation. Contrairement aux deux précédentes révolutions industrielles, il semble que l'homme n'ait pas été l'acteur de cette révolution incomparable, comme si l'intelligence artificielle avait déjà pris le dessus… Il lui faut reprendre son cerveau en main. La cybersécurité est sa chance.

Notes

1. Avec, par exemple, la nomination de Jean-Yves Latournerie, préfet chargé de la lutte contre les cybermenaces au ministère de l'Intérieur.

2. Voir le guide d'hygiène informatique de l'Agence nationale de la sécurité des systèmes d'information (Anssi), janvier 2013, disponible en ligne : http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf

3. Voir "2014 Data Breach Investigations Report", Verizon, 2014 (http://www.verizonenterprise.com/fr/DBIR/2014/), et "Internet Security Threat Report 2014", vol. 19, Symantec, avril 2014 (http://www.symantec.com/fr/fr/security_response/publications/threatreport.jsp).

4. Phishing *: hameçonnage par un leurre figurant en pièce jointe ou en lien actif dans un mail dit « pourriel ».*

5. Watering Hole *: technique de l'attaque de point d'eau.*

6. Bitcoin : « cryptomonnaie ». Voir aussi la définition du lexique financier en ligne des Échos *: http://www.lesechos.fr/finance-marches/vernimmen/definition_bitcoin.html*

7. Voir, par exemple, le site Pastebin.com.

8. DDoS : Distributed Denial of Service *; une attaque DDoS est une attaque par déni de service distribué.*

9. APT : Advanced Persistent Threat *; il s'agit d'une attaque sournoise et persistante dans le SI, non détectée rapidement.*

10. Ou extraction de données des systèmes de traitement automatisé de données depuis la loi du 13 novembre 2014.

11. Articles 226-17 et 226-17-1 du Code pénal (34 et 34 bis de la loi de 1978).

12. Art de faire parler les gens sous de faux prétextes en exploitant les failles humaines (curiosité, naïveté, rancœur, jalousie, cupidité, ego, peur).

13. « Sécuriser une architecture de téléphonie sur IP », note technique de l'Anssi, 23 décembre 2013 : http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_securiser_ToIP_NoteTech-v1.pdf

14. « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé », note de transmission de la Communauté européenne, février 2013 : http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=fr

15. « Rapport "Protéger les internautes" : vers une chaîne interministérielle de lutte contre la cybercriminalité », éditorial de Myriam Quéméner, Observatoire-fic.com, 8 septembre 2014 : http://www.observatoire-fic.com/edito-rapport-proteger-les-internautes-vers-une-chaine-interministerielle-de-lutte-contre-la-cybercriminalite-par-myriam-quemener-avocat-general/

16. GAFA : Google, Apple, Facebook, Amazon.

17. The USA Patriot Act : http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact

18. DSI : directeur des systèmes d'information. RSSI : responsable de la sécurité des systèmes d'information. CIL : correspondant informatique et libertés.

19. Présentation du colloque du 18 novembre 2014 organisé par l'Adij, le Cercle Montesquieu et CA Technologies sur le thème « Les entreprises face aux cyber-risques : état des lieux et perspectives » : http://www.adij.fr/2014/11/08/colloque-les-entreprises-face-aux-cyber-risques-etat-des-lieux-et-perspectices/

20 . La sécurité by design *signifie que la notion de sécurité est prévue dès la conception d'un logiciel ou d'un produit pour assurer la cybersécurité.*

21. « Cyberattaques : une facture de 4,8 M€ par entreprise en France », par Ariane Beky, article publié le 24 octobre 2014 sur Silicon.fr : http://www.silicon.fr/cyberattaques-entreprise-france-2014-100144.html

22. Voir le rapport d'information du Sénat (http://www.senat.fr/rap/r07-449/r07-4496.html) ainsi que le compte rendu de l'audition publique du 21 février 2013 sur le thème « Le risque numérique : en prendre conscience pour mieux le maîtriser » (http://www.senat. fr/compte-rendu-commissions/20130218/etr.html#toc7)

23. À propos de la nouvelle France industrielle : http://www.entreprises.gouv.fr/politique-et-enjeux/la-nouvelle-france-industrielle

24. Lire le compte rendu du CyberCercle du 7 mai 2014 sur le thème « La nouvelle France industrielle : feuille de route du plan Cybersécurité (plan 33) » : http://www.defense-et-strategie.fr/index.php?option=com_ content&view=article&id=553:cybercercle-du-7-mai-2014-la-nouvelle-france-industrielle-feuille-de-route-du-plan-cybersecurite-plan33&catid=114:le-cybercercle&Itemid=367

25. « "La cybersécurité est une question de souveraineté", selon Guillaume Poupard », par Patrick Déniel et Hassan Meddah, article publié sur Usine-digitale.fr le 22 mai 2014 : http://www.usine-digitale.fr/article/la-cybersecurite-est-une-question-de-souverainete-selon-guillaume-poupard.N264163

26. Lire l'entretien avec Thierry Delville, délégué aux industries de sécurité, publié sur le site de l'Union des entreprises de sécurité privées (USP) le 10 novembre 2014 : http://usp-securite.org/entretien-avec-thierry-delville-delegue-aux-industriels-de-securite/

27. CERT : Computer Emergency Response Team *(privé ou public) ; www.cert.ssi.gouv.fr*

28. Loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, loi sur les atteintes aux systèmes informatiques (dite « Godfrain ») du 5 janvier 1988 et loi pour la confiance dans l'économie numérique du 21 juin 2004.

29. Notamment dans le Code des postes et des communications électroniques (CPCE) et le Code de la propriété intellectuelle (CPI).

30. « Proposition de règlement sur la protection des données : ne pas hypothéquer la croissance de l'économie de demain », document publié en ligne par le Syndicat des régies Internet (SRI) et l'Interactive Advertising Bureau (IAB) France : http://www.sri-france.org/wp-content/uploads/2014/12/26-09-2014-IAB-FRANCE-SRI-Position-donnes-personnelles.pdf

Bibliographie

MINC A. ; NORA S., *L'informatisation de la société*, La Documentation française, 1978.

ROBERT M., « Protéger les internautes. Rapport sur la cybercriminalité », rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014. Disponible en ligne : http://www.justice.gouv.fr/ include_ htm/pub/rap_cybercriminalite.pdf

SOUVIRA A., « Du rapport Nora-Minc à la lutte contre la cybercriminalité », *La Revue du Grasco*, n° 8, février 2014, p. 11. Disponible en ligne : http://fr.slideshare.net/sebastiendupent/revue-n8-fevrier2014

Du risque informatique au risque sociétal

The SnowCrew

Hacker

En se jetant à corps perdu dans la révolution numérique, le monde des entreprises a pensé, un temps, la mettre à son service. Puis il a réalisé, plus récemment, que l'Église catholique avait eu en son temps le même dessein concernant l'imprimerie de Gutenberg. Pour mémoire, l'impression de la Bible et la circulation accélérée des textes sacrés dans des langues vernaculaires ont provoqué, au fur et à mesure de l'alphabétisation des populations, la montée en puissance d'une critique du système en place, qui allait finir par se révéler propice au développement du protestantisme et, d'une certaine façon, du capitalisme.

C'est à ce type de bouleversement systémique qu'est confronté le monde avec le numérique, et cette grande redistribution des cartes qui a à peine commencé laisse apparaître de nouvelles figures du pouvoir, parmi lesquelles les mystérieux hackers.

Sony, Orange, JP Morgan, ou plus récemment TF1, les grandes entreprises victimes d'attaques informatiques sont légion, et la quantité de données dérobées tient plus de l'avertissement clair et net que de la répétition de signaux faibles : ce qui pourrait apparaître comme une malencontreuse succession d'actes de délinquance n'est en réalité qu'un théâtre d'ombres dans la caverne où sont enfermés ceux qui n'ont pas saisi le rôle grandissant que les hackers sont appelés à jouer sur la scène politico-économique.

Quand les hackers entrent en scène

Le phénomène hacker le plus disruptif de ces dernières années, celui qui a marqué un basculement politique évident, est sans conteste le célèbre WikiLeaks. Si Julian Assange est connu des initiés pour avoir, dès son adolescence, utilisé le hacking à des fins politiques – il protestait alors contre la prolifération des armes nucléaires –, c'est avec WikiLeaks qu'il a posé celui-ci comme acte politique majeur, en modifiant de façon durable l'équilibre des forces entre populations civiles et gouvernements et en imposant ce que beaucoup qualifièrent alors de « dictature de la transparence ».

Redistribution du pouvoir politico-économique

WikiLeaks a ainsi ouvert la voie au courant des *whistleblowers* (« lanceurs d'alerte »), qui n'arrête pas depuis de faire des émules, d'Edward Snowden, qui, après Bradley Manning, a achevé de réduire à peau de chagrin l'image vertueuse de la démocratie américaine, aux récents LuxLeaks, qui ont dénoncé les montages fiscaux mis en place par le Luxembourg de Jean-Claude Junker et détruit les espoirs que de nombreux citoyens plaçaient dans les institutions européennes. « Hacker » les circuits informationnels qui alimentent une confiance que des individus comme Julian Assange jugent usurpée et dévoyée, c'est le cœur de l'action politique des partisans de la transparence et c'est le moteur d'une vaste redistribution du pouvoir politique.

Personne mieux que Hans Christian Andersen n'a à ce jour résumé de façon plus limpide le rôle politique joué par les hackers dans ce XXIe siècle qui commence. Dans *Les habits neufs de l'empereur* (1837), le conteur narre l'histoire d'un empereur, plus soucieux de ses toilettes que des affaires du royaume, acquérant auprès d'escrocs une étoffe censée avoir la propriété de n'apparaître comme transparente qu'aux yeux des usurpateurs. Ne la voyant pas lui-même mais apeuré à l'idée d'être démasqué en tant qu'imposteur, le roi s'en drape et parcourt sa ville sous le regard médusé de son peuple qui n'ose dire un mot, jusqu'au moment où un enfant innocent s'écrie : « Le Roi est nu. »

Remplacez le roi par les gouvernances – étatiques ou corporate –, ses toilettes par la communication et le marketing, l'étoffe par les technologies Internet qui régissent désormais le monde, l'enfant innocent par une partie grandissante de la population, et vous avez là une allégorie parfaite du climat politico-économique contemporain. Les tisserands qui ont mis au point l'étoffe magique, dans cette histoire, sont – vous l'aurez deviné – les hackers, car, pour ceux qui auraient raté un épisode datant des années 1970, l'Internet a été mis au point par des hackers.

Une responsabilité à assumer pour les entreprises

C'est bien aux gouvernances de tout poil que les hackers promettent un voile de transparence qui les rendra, aux yeux de ceux sur lesquels ils régnaient naguère en toute légitimité, nus comme un enfant qui vient de naître – ou, plus exactement, comme le portrait de Dorian Gray. Une nudité qui fera apparaître au grand jour le rôle éminemment politique joué par les grandes entreprises dans la marche du monde et les placera dans une position si inédite dans la culture française qu'il faut, pour la décrire, emprunter à la langue de Shakespeare un mot qui n'a pas pour le moment d'équivalent en français : *accountability*.

Un risque aux frontières poreuses

Le risque en matière de sécurité informatique est donc bel et bien et avant tout un risque politique, dont la dimension économique n'est qu'un effet de bord. Le risque pour toute entreprise confrontée à une telle attaque est de se retrouver dans la situation inconfortable d'un responsable politique vis-à-vis de consommateurs qui se révèlent être, en fin de compte, des citoyens. Pour appréhender ce risque, il est devenu indispensable – en dehors d'accorder des budgets suffisants à la sécurité informatique – de l'anticiper et de le comprendre finement, non pas dans sa dimension technique, ou pas seulement, mais aussi et surtout dans ses dimensions politique, sociale et culturelle. Il convient également de faire le deuil de l'idée d'une sécurité parfaite. Au cas où la National Security Agency (NSA) ne vous aurait pas convaincu, cela n'existe pas : on peut réduire ce risque, mais on ne peut en aucun cas l'éliminer.

Le Lulz, une culture et un risque

Les hackers sont par ailleurs, dans la société panoptique mise en place par de nombreux États

occidentaux, les seuls à être en mesure d'échapper à Big Brother, ce qui leur confère de facto, à l'heure où, en France comme ailleurs, la cybersurveillance est mise au service de la lutte contre toute forme de contestation sociale, les fonctions cumulées d'un Bob Woodward (le journaliste du Watergate) et d'un Che Guevara.

Les efforts maladroits du pouvoir pour décrédibiliser ce mouvement – qui s'apparente à une lutte à mort contre la marée montante – n'ont mené qu'à l'installation de celui-ci dans une position de chevalier blanc des temps modernes. Cela s'illustre dans le harcèlement judiciaire dont est victime Julian Assange, qui a fait de lui le symbole d'une génération tout entière, dans la lutte contre le téléchargement illégal, sacralisant les « pirates » dans le rôle de Robin des bois du cyberespace, ou bien encore dans l'attribution par le gouvernement américain des attaques ayant visé Sony à la Corée du Nord. Unanimement dénoncé par les spécialistes comme une supercherie et prouvé comme telle dans les jours qui suivirent, ce mensonge dans lequel s'est enfoncé Barack Obama, encore moins convaincant que celui d'un Saddam Hussein et ses prétendues armes de destruction massive, apparaît jour après jour comme une énième tentative de construction d'un ennemi censé souder le camp du bien contre celui du mal.

Face à l'injonction paradoxale

Mais, si les États disposent – en dernier recours – de la violence légitime qui leur permettra, quitte à enterrer toute illusion démocratique, de se maintenir en place, il en est tout autrement des entreprises, qui n'ont à ce jour pas trouvé, à de rares exceptions près, le moyen d'imposer à leurs consommateurs d'acheter leurs produits. Témoin le flux d'informations mêlant Coca-Cola à Israël qui a envahi les réseaux sociaux l'été dernier et causé un effondrement des ventes de l'entreprise dans le monde arabe, ou bien encore celui dénonçant les pratiques sociales de la même entreprise en Espagne et qui ont eu, dans tout le pays, le même effet. Car si le hacking était naguère cantonné aux territoires des technologies, il est depuis Julian Assange – qui se revendique par ailleurs journaliste – étendu au territoire bien plus vaste, et ô combien plus visible, de l'information en général.

Les entreprises n'ont pas le choix, elles vont devoir composer avec un monde qui change et trouver un moyen de cohabiter avec le phénomène hacker et son extension au territoire de l'information. Par ailleurs, elles vont devoir survivre à l'une des conséquences immédiates du phénomène : la multiplication des attaques informatiques. Certaines, comme Sony (1), s'exposeront même au risque de devenir, au fil des attaques, la tête de Turc des hackers. Au fur et à mesure des attaques, les entreprises réaliseront le « paradoxe WikiLeaks », l'injonction paradoxale introduite par la « dictature de la transparence », selon lequel il est indispensable qu'une information circule de façon rapide et efficace pour qu'elle crée de la valeur ajoutée dans une entreprise, le risque de voir cette information « fuiter » étant proportionnel à l'ampleur de sa circulation. Tout frein à cette circulation – revenir aux fax et à la machine à écrire pour limiter les attaques informatiques – ferait inexorablement chuter la productivité d'une entreprise, la mettant à la merci de la concurrence, et toute accélération de cette circulation ferait grimper le risque de fuite. Une baisse de productivité n'étant pas envisageable, c'est assez naturellement vers la maîtrise du risque que les entreprises vont se tourner, ainsi que son corollaire : l'assurance.

Le cyberespace, un territoire encore inconnu

Les entreprises sont passées, en une décennie à peine, d'une appréhension de la « révolution numérique » comme – au départ – d'un « canal de vente complémentaire » ou – pire encore – d'un « média » qu'il s'agissait de maîtriser, à une approche plus nuancée faite de craintes et de doutes en grande partie dus à une méconnaissance profonde du sujet. Si les risques existent bel et bien, c'est en les comprenant finement et en les abordant

non seulement dans leur dimension technologique mais également dans leurs dimensions politique et culturelle que l'on peut avancer dans ce territoire nouveau qu'est Internet.

Il fut un temps où la Chine représentait pour les acteurs économiques un eldorado, puis le pays se transforma en cauchemar dans lequel de nombreuses entreprises françaises s'étaient perdues, avant que tous ne réalisent qu'il s'agissait là d'une culture riche et complexe, mais ô combien différente de celle à laquelle nos entreprises étaient habituées, et que débarquer dans ce pays de façon conquérante était voué à un échec cuisant. Il en est de même avec Internet. Après une période d'euphorie à laquelle a succédé un climat anxiogène entretenu par des politiques qui voient – à juste titre – dans Internet une menace à leur légitimité, il est temps de prendre du recul et d'aborder ce nouveau territoire comme une terre étrangère dotée d'une culture spécifique et habitée par d'étranges créatures – les internautes – qui ne sont que les projections, souvent partielles, parfois extrêmes, d'êtres humains venus de toutes parts et transcendant bien des frontières. Car, si les frontières existent dans le monde réel, elles semblent parfaitement arbitraires et totalement inutiles dans le cyberespace.

Comprendre – au sens étymologique – tout cela est une étape indispensable pour en tirer parti et en profiter demain.

Note

1. En 2011, Sony a été victime d'une attaque qui lui a coûté des dizaines de millions de dollars et qui a fait plonger sa valorisation boursière de plus de trois milliards de dollars.

Transformation numérique et sécurité deux faces d'une même pièce

Jean-Paul Mazoyer

Directeur informatique et industriel Groupe, Crédit Agricole SA

La cyberdéfense est un sujet d'actualité, mais les établissements financiers sont, depuis longtemps, sensibles à la question. Le bon sens, parce que la matière première d'une entreprise du tertiaire est l'octet, et l'expérience des services en ligne ont apporté un niveau de sécurité adapté aux menaces présentes. Mais nous verrons que les défis sont nombreux et imposeront une intensification des efforts, non seulement d'ordre technique mais aussi du point de vue organisationnel, voire culturel.

Un contexte en plein changement

La logique de sécurité a été, pendant longtemps, axée sur la prévention de l'utilisation frauduleuse et sur la disponibilité du système d'information (SI). Il s'agissait d'éviter qu'un utilisateur autorisé, à tort ou à raison, n'accède à une application financière et l'utilise à son profit.

Il en découla très logiquement une sécurisation basée sur deux principes : d'une part, éviter que des personnes extérieures à l'entreprise puissent atteindre les applications internes et, d'autre part, assurer une gestion très serrée des droits d'accès.

Restait alors à limiter les risques de fraude par une séparation des pouvoirs et un renforcement des contrôles.

Mais l'environnement change rapidement depuis quelques années. La partie adverse s'est organisée et industrialisée. Des savoir-faire technologiques connus de quelques personnes dans les années 1990 se sont largement vulgarisés. Aujourd'hui, il y a clairement un modèle quasi industriel visant à ratisser beaucoup plus efficacement le cheptel des entreprises vulnérables. Des chercheurs de vulnérabilités commercialisent le fruit de leurs recherches. Ces vulnérabilités sont soit incluses dans des packages de programmation, eux-mêmes repris par des « éditeurs » de chevaux de Troie commercialisant leur création auprès de ceux qui les déploieront par centaines de milliers et vendront à leur tour leurs réseaux de PC asservis pour mener des attaques, soit achetées à prix d'or par des organisations recherchant une approche plus discrète.

La technologie employée par les fraudeurs a été forgée pour échapper à la vigilance des panacées d'hier que sont les logiciels antiviraux et les systèmes de filtrage Internet. La lutte anti-*malware* (1) n'est

donc plus aussi simple que par le passé : omniprésence des antivirus et tenue à jour de leur base de signature restent nécessaires mais ne sont qu'un des éléments du dispositif.

Autre aspect : les réseaux hostiles peuvent se targuer d'une impunité quasi totale car ils jouent sur une très forte répartition des rôles et des moyens hors de nos frontières, et il faut bien admettre que la coopération internationale se concentre davantage, à juste titre, sur le traitement des délits portant gravement atteinte aux personnes.

Enfin, les organisations parallèles se sont construit des marchés de négoce des biens immatériels volés. Des places de marché occultes, qui fleurissent sur un réseau (TOR (2)) impénétrable initialement conçu pour des actions louables (liberté d'expression, protection de la vie privée, etc.), facilitent grandement la revente de tout objet, physique ou virtuel, illicite.

En synthèse, les technologies d'infiltration des fraudeurs permettent d'aller chercher des données (du simple nom au numéro de Sécurité sociale en passant par la donnée de carte bancaire) au sein des entreprises en vue de les exploiter directement (utilisation des numéros de carte bancaire, demande de rançon) ou de les revendre à ceux qui, à leur tour, les exploiteront. En outre, des moyens considérables de saturation des équipements Internet des entreprises sont mis en location sur les mêmes marchés.

Le changement qui s'opère du côté hostile va de pair avec, du côté des entreprises, un appétit croissant pour la nouveauté. La fameuse transformation digitale dont il est question dans tout le secteur tertiaire recherche un meilleur partage de l'information (*big data*), qui passe par des extractions et des mises à disposition auprès d'analystes, un enrichissement fonctionnel des services auxquels peuvent accéder les clients (communication, opérations disponibles, souscription de contrat), les collaborateurs et les entreprises, une plus grande diversité des moyens d'accès au SI, un recours intensif au réseau Internet en tant que liaison et un grand appétit pour les solutions « clés en main » proposées dans le *cloud*. Cela pourrait constituer une conjonction catastrophique s'il n'était pas prévu d'associer à la « transformation digitale » une dimension sécuritaire intégrée dès le départ.

Un réalignement nécessaire de capacités existantes

Conception des offres

Sur le plan de la conception des offres, l'ère actuelle confirme l'intérêt de l'analyse de risque associant les métiers et les fonctions support (informatique, back-office, etc.) plutôt qu'une approche par la pure conformité à des politiques de sécurité. De manière générale, le fameux « cycle en V » (un enchaînement linéaire de phases de spécifications, réalisation et recette) est désormais jugé inadapté au besoin actuel de créativité et d'amélioration continue. L'approche régissant la sécurité d'une offre par l'application rigide d'une politique de sécurité relève de ce même « cycle en V ». Il faut donc analyser l'offre en cours de conception avec quelques fondamentaux en tête : primo, il faut considérer la sécurité dans son ensemble, de l'authentification (ou non) de l'utilisateur jusqu'au traitement de sa demande dans les back-offices et les systèmes en sortie de la chaîne des traitements ; secundo, face au foisonnement des fonctionnalités proposées, il faut veiller à ce qu'elles ne soient pas grossièrement contournables puis mettre en place une capacité d'observation en « temps réel » des usages, associée à une capacité réelle de réaction (correction, voire fermeture du service détourné de sa finalité prévue).

La conception des applications et des systèmes sur lesquels elles s'exécutent doivent tenir compte d'une capacité d'infection quasiment biologique de tout ce qui est plongé dans l'Internet. À cela s'ajoute la nécessité de considérer qu'un *malware* introduit dans l'entreprise amènerait une capacité d'attaque sur des ressources internes.

Il nous faut revoir notre rapport aux données et réévaluer la préciosité de celles-ci. La feuille de calcul ou la base de données auxiliaire constituées à l'occasion d'une étude marketing ponctuelle peuvent se révéler être une mine d'or pour celui qui réussirait à se les approprier. Il y a une « hygiène » à redéfinir et à réévaluer en réponse à la nouvelle valeur acquise par les données sur les marchés occultes. Cette hygiène « 2.0 » doit englober la délicate question du stockage « hors » des murs de l'établissement (recours aux offres externalisées, en particulier au *cloud*) à examiner au cas par cas, selon la nature des données et selon la possibilité d'une neutralisation préalable des données (anonymisation, chiffrement).

Ressources technologiques

Du côté de la technologie, il s'agit d'admettre que quelque chose de nouveau, inconnu des systèmes de prévention, ait pu s'infiltrer au cœur de l'entreprise. On pourrait s'étonner qu'une telle hypothèse puisse être envisagée, mais prévoir le pire n'a rien de condamnable. Dans le monde physique, la prévention et l'éducation n'ont pas éliminé le besoin de détecteurs d'incendie et de pompiers !

Nos informatiques doivent s'équiper en ressources technologiques et en compétences nouvelles pour détecter toujours mieux les activités atypiques, non seulement au niveau des applications sensibles, comme par le passé, mais aussi au niveau des ressources élémentaires : accès massif à des fichiers par ce qui semble être un utilisateur autorisé, flux anormal de données en sortie, etc. Nous considérons que cette capacité de détection doit être développée en étroite concertation avec les métiers qui sont les seuls à connaître l'usage normal de leur SI.

Cette capacité de détection passe par le déploiement d'équipements émetteurs d'alerte et la génération de messages dont l'analyse, si possible immédiate, est un défi sans cesse renouvelé. La technologie devra aussi proposer des solutions en réponse au besoin d'élargissement et d'intensification de la protection des données. Cela passe par un développement des moyens cryptographiques. Rien de nouveau pour des établissements familiers des standards les plus exigeants en matière de protection des données de carte bancaire (PCI-DSS) mais un élargissement à des données plus « banales ».

Les infrastructures de gestion des éléments cryptographiques seront mises à profit et rentabilisées par une multitude d'usages : authentification non rejouable, reconnaissance des serveurs entre eux, scellement des transactions (rendant ainsi impossible leur modification après émission de l'ordre initial). Les ateliers de développement auront à généraliser le recours aux meilleures techniques de sécurisation des développements. La menace, hypothétiquement devenue intérieure par rebond, peut s'exercer sur des applications à usage interne. Sans une montée homogène de niveau, une application très auxiliaire pourrait devenir une source d'informations qui permettraient ensuite de contourner les protections d'une application plus sensible.

Les établissements ont depuis longtemps envisagé les pires avanies. Notamment, la question des désastres physiques est traitée depuis des décennies, question de bon sens mais aussi de réglementation. La notion de désastre logique est abordée sous l'angle de la continuité « ordinaire » de la production informatique, mais le traitement d'un cyber-ravage massif nous amène à envisager la reconstruction simultanée d'ensembles fonctionnels distincts. De même, les établissements ont constitué des centres de secours leur permettant d'assurer la conduite des activités essentielles en cas de dommages majeurs à un bâtiment, voire un groupe de bâtiments. Il s'agit aujourd'hui de s'assurer que ces centres de secours resteraient opérationnels en cas de destruction d'un composant vital du réseau de PC (réseau local, annuaire central, etc.).

On voit ainsi se rapprocher la sécurité des SI et la problématique du plan de continuité des activités. Ici encore, synergies et agilité sont de mise.

Toujours du côté de la technologie, le sujet de la dépendance à l'égard d'Internet s'impose. Ce réseau, dont le pilotage et l'administration s'appuient sur une

très forte diffusion des moyens techniques et des responsabilités, fait preuve d'un taux de disponibilité admirable. Mais deux catégories d'événements peuvent noircir le tableau : Internet peut faire l'objet d'attaques sévères visant à en déstabiliser le fonctionnement à l'échelle mondiale ou régionale (attaques portées à des infrastructures vitales), et les points de raccordement des entreprises peuvent, eux aussi, faire l'objet d'attaques (notamment par déni de service, des centaines de milliers de PC asservis se connectant simultanément aux ressources pour les saturer).

Nos entreprises n'ont strictement aucune prise sur la première catégorie et devraient subir l'absence transitoire d'Internet. C'est à méditer en cas d'appui d'activités vitales sur ce réseau (au-delà de la messagerie et du surf, l'accès aux CRM (3) externalisés, aux systèmes d'impression sous-traités, etc., doit faire l'objet d'une grande attention et d'une définition de procédures de contournement).

En revanche, elles doivent s'adapter à la seconde catégorie, qui n'a rien d'une fiction. Les dispositifs d'écrêtage font leurs preuves dans des attaques massives, mais ils sont coûteux et doivent être pris en compte dans l'équation budgétaire que l'on établit lorsqu'un recours au *cloud computing* est envisagé.

L'évolution des compétences

Sur le plan des compétences, l'évolution de la nature des menaces et de leur intensité remet beaucoup de choses en question. Il est bien dommage d'en être arrivé là mais, outre une sensibilisation à la valeur des données et la nécessité de bien concevoir les produits, il va falloir développer une culture de la méfiance. L'art des fraudeurs est passé en quelques années de l'âge de pierre à l'ère spatiale. Pas d'exception dans le ratissage qui s'opère actuellement. L'ingénierie sociale qui consiste à accumuler de l'information sur l'entreprise et une partie de son organisation puis à influencer un collaborateur pour lui faire commettre une erreur est facilitée par l'abondance d'informations disponibles sur les réseaux sociaux et la propension des entreprises à publier largement leurs organigrammes, leurs répertoires et moult détails sur leur fonctionnement et leurs projets en cours. Après avoir créé un contexte de confiance (courriels préalables, conversations téléphoniques avec des références nombreuses à des personnes, des projets, des hobbies), l'attaquant va obtenir une transaction financière en sa faveur ou bien l'installation d'un logiciel de prise de contrôle à distance (cheval de Troie). Il y a donc une sensibilisation, pour ne pas dire une véritable éducation à généraliser dans nos entreprises.

D'autre part, nous manquons d'architectes de solutions de sécurité, de spécialistes des tests d'intrusion, de personnes maîtrisant la chaîne fonctionnelle de bout en bout. Cette situation fait que les intervenants traitent les sujets en silo, ce qui aboutit à des juxtapositions de solutions de sécurité visant chacune à traiter la problématique de la sécurité dans son intégralité. Ces approches dépassées mais encore fréquentes alimentent l'idée d'une sécurité dogmatique, contre-productive, antinomique de l'innovation. On commence à percevoir la nécessité d'une transversalité dans le domaine de la gestion de données (*chief data officer*) et de la transformation digitale (*chief digital officer*), mais nous avons du mal, malgré une grande antériorité, à valoriser une fonction sécurité orientée « métier ». Chaque établissement aura à réfléchir à ces questions de formation et de transversalité. Les modèles d'organisation abondent, mais aucun ne parvient vraiment à faire décoller une nouvelle approche.

Autre défi : la montée en compétence des informaticiens encore très réticents à recourir à la cryptographie (chiffrement, scellement), perçue comme complexe et source de perturbation des opérations (clés manquantes, perte de performance). Ne nous leurrons pas, la cryptographie est un domaine complexe, et le design d'une application intégrant la cryptographie demande une compétence pointue, donc rare, que l'on concentre de ce fait sur les zones les plus sensibles (systèmes de paiement notamment).

Nous voyons donc que la formation et la sensibilisation conditionnent l'adaptation des entreprises au

développement de la cybermenace. S'en convaincre est une chose ; déclencher une prise de conscience et une adhésion au niveau des directions des ressources humaines en est une autre tant le sujet semble rébarbatif aux non-initiés. Simple question : combien de stages de management comportent-ils un volet relatif à la protection de l'information ?

Une transformation raisonnée

Autre point : les entreprises actuelles font partie d'un tissu économique complexe que l'on pourrait qualifier d'écosystème. Cela signifie que, quel que soit leur avancement en matière de cybersécurité, des dépendances complexes offrent des moyens de contournement aux attaquants. L'actualité des dernières années a bien montré qu'une entreprise certifiée comme répondant aux standards de sécurité les plus exigeants peut se faire attaquer via un fournisseur dont la vocation est lointaine de l'objet de la fraude : un fournisseur de systèmes de conditionnement d'air, un opérateur de l'équipement multimédia d'un amphithéâtre, un opérateur de gestion technique de bâtiment, voire même un fournisseur de systèmes de contrôle d'accès.

L'entreprise souhaitant maîtriser sa sécurité devra passer par une urbanisation stricte des points de contact avec les entreprises tierces, dont il faudra limiter l'accès dans le mode « tout ce qui n'est pas autorisé est interdit ». Cette approche apportera un premier niveau d'élévation de la résistance.

Cela étant, on n'échappera pas à l'impérieuse nécessité de voir l'intégralité des acteurs économiques atteindre un niveau de sécurité homogène. En effet, qu'une entreprise s'isole de son opérateur de télécommunications n'a pas de sens ! C'est pour cette raison que les initiatives de l'État – loi de programmation militaire, future directive européenne sur la sécurité des réseaux et de l'information (SRI) – doivent être vues comme une opportunité et non uniquement comme une servitude, si tant est qu'elles ne perdent pas de vue leur visée initiale (une montée globale de la sécurité du tissu économique et non une surfocalisation sur quelques bons élèves).

Il est aisé de comprendre que la progression d'ensemble sera lente, car le sujet est complexe et chacun aura sa vision des priorités.

La complexité du sujet au niveau de l'entreprise, son caractère transsectoriel, l'agilité et l'inventivité de la partie adverse, le fait que nous soyons placés dans la logique du défenseur d'une forteresse tentaculaire virtuelle dont une seule faille peut donner l'avantage à l'ennemi nous amènent à la question cruciale de la gestion de crise et de la reconstruction (déjà évoquée ci-dessus). Nos entreprises, dirigeants inclus, doivent définir puis tester leurs processus décisionnels, leur communication pour minimiser l'expansion d'un problème, démontrer la maîtrise de la situation et éviter les effets de panique.

Il est impossible de terminer ce panorama sans parler du contrôle. Nous avons évoqué la multiplicité des rouages à agencer pour élever et adapter constamment le niveau de sécurité de l'entreprise. Nous avons constaté que des politiques de sécurité statiques ne permettaient plus de faire face au besoin d'innovation des clients et des métiers, à l'évolution rapide des offres de service (*cloud*) et à l'inventivité des attaquants. Dans ces conditions, on peut s'interroger sur les modalités du contrôle. Traditionnellement appuyé sur des check-lists et un délai d'actualisation d'un an, le contrôle risque de se trouver très déphasé par rapport à la complexité de la situation et sa rapide évolution. D'autre part, la question de la meilleure allocation des trop rares compétences en sécurité des SI se pose crûment : construire la défense ou contrôler les constructeurs ? Ce débat mérite d'être formalisé pour aboutir rapidement à des synergies et à un contrôle, adaptatif dans le temps, qui contribuerait activement au pilotage.

En conclusion, la démonstration est faite que la transformation digitale de l'entreprise doit intégrer d'emblée la dimension sécuritaire dans tous les domaines : conception des produits, construction

et pilotage des infrastructures, formation et sensibilisation, gestion de crise, modalités de contrôle. Nouveaux métiers, nouvelles approches, nouvelle mentalité. Et puisque la somme des transformations numériques des entreprises se traduit par une transformation numérique de la société dans son ensemble, l'État (superviseur) a un rôle à jouer selon des modalités à réinventer.

Notes

1. Malware *: « logiciel malveillant ».*

2. TOR : The Onion Router. *Système de routage « en oignon » qui vise à renforcer l'anonymat des informations circulant sur les réseaux.*

3. CRM : Customer Relationship Management*, ou « gestion de la relation client ».*

Risques et solutions de cybersécurité

Alain Bénichou

Président d'IBM France

Agnieszka Bruyère

Directrice des services de sécurité, IBM France

La sécurité représente l'une des cinq initiatives stratégiques d'IBM (1) *établies par notre chairman et CEO Ginni Rometty. La transformation de l'entreprise implique un changement du paradigme en matière de sécurité : elle ne peut plus être considérée comme un château fort mais plutôt, si l'on fait le parallèle avec un être vivant, comme un système immunitaire. Notre engagement dans le domaine de la sécurité est de conseiller les entreprises, institutions et gouvernements du monde entier sur la manière de protéger leur organisation des menaces et de proposer à nos clients l'offre et les services de sécurité les plus complets de l'industrie.*

Pour ce faire, IBM a investi plusieurs milliards de dollars dans la constitution d'une division de sécurité dédiée, l'acquisition de sociétés de sécurité parmi les plus prisées du marché (ex : Trusteer), dans un réseau de centres opérationnels de sécurité de pointe, dans la recherche et le développement pour innover dans des solutions de sécurité, et enfin, dans la constitution d'une plateforme d'intelligence de sécurité au service de ses clients.

La multiplication des menaces de sécurité engendre un coût sans cesse croissant pour l'ensemble des organisations. La réponse à cet enjeu devient stratégique et passe par la prise en compte de plusieurs domaines :

- *la gestion des facteurs humain et organisationnel (éducation comportementale, automatisation des processus quand cela est possible) ;*
- *l'anticipation, la détection et la gestion des attaques par des solutions ciblées de type « Advanced Threats Intelligence Service » (service d'intelligence relatif aux menaces avancées) et « SIEM : Security Information and Events Management » (Gestion des informations et des événements de sécurité) ;*

- *la protection des données critiques, qui devront préalablement être identifiées puis localisées avant de pouvoir être sécurisées par des solutions adaptées ;*
- *la sécurisation des applications dès la conception puis par contrôle continu ;*
- *la protection anti-DDoS (déni de service distribué).*

La multitude des initiatives dans ce domaine rend nécessaire la création d'un réel programme de sécurité au sein de l'entreprise qui permettra de donner une vision intégrée en matière de sécurité.

Ces derniers mois, la presse s'est largement fait l'écho de l'augmentation des failles de sécurité visant les entreprises dans de nombreux secteurs. Ces failles de sécurité ont non seulement entraîné des dépenses importantes dans les entreprises visées, mais ont aussi impacté considérablement la confiance des consommateurs et la réputation des marques. Le sujet de la sécurité n'est plus désormais sous la seule responsabilité de la DSI, il est dorénavant une priorité incontestée des dirigeants de l'entreprise. Les organisations doivent évoluer vers une approche plus systématique et proactive pour répondre aux menaces en matière de sécurité et aux exigences réglementaires dans l'économie actuelle, centrée sur l'information.

Une étude récente du cabinet Ponemon Institute® (2) a montré que le coût moyen d'une perte de données clients est de 206 dollars par personne pour les banques, et que le coût direct moyen d'un incident, toutes industries confondues, est de 3,5 millions de dollars.

Avec des sommes aussi importantes, les professionnels du secteur informatique, les dirigeants, les chefs d'entreprise ont besoin de mieux connaître les causes et les conséquences financières de ces incidents, y compris le coût d'une atteinte à la réputation et à la valeur intrinsèque d'une marque.

Dans un but d'efficacité dans l'affectation du budget informatique et pour favoriser les efforts déployés pour la gestion des risques, il est nécessaire de comprendre :

- quelles sont les menaces auxquelles l'organisation est exposée ;

- quel est le niveau de vulnérabilité de l'organisation face à ces menaces ;

- quelles pourraient être les conséquences d'une attaque en termes de défaillances informatiques (des interruptions d'activité) ou de vols de données ;

- quel serait le coût d'une telle attaque en tenant compte des coûts directs (coût de rétablissement du fonctionnement du système d'information, coût des investigations, coût de notification aux victimes, etc.) mais également des coûts indirects tels que l'impact sur la réputation, la perte de recettes due à des indisponibilités des systèmes, le coût de non-respect de certaines exigences juridiques et réglementaires.

Ces éléments permettent d'évaluer les risques de l'organisation en matière de cybersécurité, d'établir les priorités et d'identifier des projets pertinents pour assurer la sécurité informatique.

Cette analyse des risques doit être effectuée au niveau de chaque entreprise, et ses conclusions seront spécifiques à chacune d'entre elles. Cependant, fort de notre expérience en matière de gestion des risques et plus particulièrement des cyber-risques, nous avons identifié les domaines prioritaires pour diminuer l'exposition de l'entreprise aux risques informatiques : 1. le facteur humain ; 2. l'anticipation, la détection et la gestion des incidents de sécurité ; 3. la protection des données les plus sensibles ; 4. la protection des

applications ; 5. la protection contre les attaques par « déni de service distribué », dites DDoS.

Gestion du facteur humain

Le facteur humain est un élément clé de la défense de l'entreprise. D'une part en raison du rôle qu'il joue dans le mode opératoire des attaquants, et d'autre part par les erreurs qu'il peut provoquer dans l'ensemble des opérations techniques qui sont confiées aux utilisateurs.

La majorité des attaques sophistiquées commencent par la prise de contrôle d'un poste utilisateur, qui va servir par la suite de base pour atteindre les systèmes et données sensibles de l'entreprise. Le moyen le plus répandu et le plus efficace de cette prise de contrôle est une attaque de type *spear phishing* (« hameçonnage ciblé »). L'attaquant va tout d'abord faire de l'ingénierie sociale : chercher les informations utiles dans les médias sociaux. Il va ensuite se servir de ces informations dans le mail qu'il va adresser à sa victime pour rendre celui-ci crédible. Le mail va contenir des liens ou des contenus malveillants, qui, par un simple clic, vont s'installer sur le poste cible. Ces logiciels malveillants sont suffisamment sophistiqués pour ne pas être détectés par un moyen de protection classique comme l'antivirus ou l'anti-*malware*.

Former

Aucune des mesures ou des solutions ne peut remplacer ce qu'IBM considère comme le socle de la sécurité des organisations : fonder une culture et un système de gestion basés sur une connaissance des risques qui commencent au plus haut niveau de la direction et qui doivent être diffusés dans toute l'organisation.

Cela implique d'identifier les sources de risque, de se fixer des objectifs et de communiquer les rôles et les responsabilités à tous les niveaux : directeurs, responsables, ainsi que l'ensemble des utilisateurs disposant d'une adresse e-mail dans l'organisation.

Cette culture passe par la mise en place de la formation continue sur les risques. Pour être pertinente, cette formation doit être basée sur des cas concrets de situation à risque, être appropriée au contexte de l'organisation et concerner directement l'individu formé.

Éviter les comportements à risque sur les réseaux sociaux

La formation est indispensable mais elle doit aller de pair avec la mise en place de solutions de protection. Il faut, tout d'abord, minimiser les risques de l'ingénierie sociale en limitant la publication de certaines informations sur les médias sociaux. Il existe des solutions de surveillance des médias sociaux à travers le compte de l'utilisateur qui permettent d'évaluer les risques découlant des informations disponibles sur ces médias. Cette solution se présente sous la forme d'une application à installer sur une tablette, un smartphone ou un poste de travail. Grâce à celle-ci, l'utilisateur autorise la surveillance des informations qu'il publie sur les médias sociaux et que les autres publient à son sujet. L'application l'avertit dans le cas où le contenu publié pourrait être exploité par l'attaquant et évalue le niveau de risque que les informations publiées représentent (par exemple, les noms des personnes mentionnées sur les médias sociaux pourraient être exploités dans l'e-mail de type hameçonnage ciblé). Cette solution porte le nom d'IBM Executive Protection® et est proposée en alliance avec la société Social SafeGuard®.

Empêcher les e-mails d'hameçonnage ciblé d'atteindre leur cible

Historiquement, les organisations ont mis en place des solutions de protection de la messagerie de type antispam. Ces solutions ne sont pas suffisantes pour empêcher les e-mails d'hameçonnage ciblé d'atteindre leur cible. Nous devons donc ajouter à ces solutions historiques des fonctionnalités contre les menaces sophistiquées et persistantes dites *Advanced Persistent Threats* (APT). Ces fonctionnalités permettent

d'analyser le contenu des mails en identifiant les liens ou un contenu malveillant grâce à la base de connaissances ou au test des fichiers attachés dans les e-mails ; elles sont disponibles chez les éditeurs tels que Proofpoint®, Websense®, TrendMicro® ou Fireeye®.

Identifier et arrêter le *malware* sur le poste d'un utilisateur

Si, malgré la formation, la protection contre les abus dans les médias sociaux et la surveillance des e-mails avec de solutions contre les APT, l'attaquant réussit à atteindre le poste de l'utilisateur, il est possible de l'arrêter grâce à la solution IBM Trusteer Apex®, qui permet de détecter, de neutraliser et de corriger efficacement les logiciels malveillants.

IBM Trusteer Apex® utilise des informations consolidées provenant de plus de vingt moteurs antivirus afin d'offrir une véritable protection et d'empêcher les fichiers malveillants connus de s'exécuter et de corrompre la machine. De plus, cette solution identifie et bloque toute connexion suspicieuse (par exemple, une connexion avec l'extérieur de l'entreprise qui serait établie par l'attaquant).

Pour conclure sur le rôle de l'individu dans la protection de l'entreprise, il faut évoquer également le risque d'erreur humaine lors des manipulations techniques. Pour minimiser ce risque, les organisations doivent envisager l'automatisation là où elle est possible.

En effet, les erreurs humaines peuvent entraîner des failles de sécurité. Pour y remédier, mettre en place des mécanismes de contrôle automatisé basés sur un système d'autorité et de droit dans la gestion des identités et des accès est plus efficace que l'utilisation par les employés de mots de passe insuffisamment sécurisés. Il faut également automatiser la gestion des correctifs de sécurité sur l'ensemble des appareils – un contrôle utilisé par seulement 51 % des organisations interrogées dans le cadre d'une étude du Ponemon Institute® réalisée pour IBM [3] –, ce qui peut contribuer grandement à répondre aux vulnérabilités en constante évolution des logiciels grâce aux solutions du marché (dont IBM QRadar QVM®).

Anticiper, détecter et gérer les incidents de sécurité

Anticiper

L'anticipation dans le domaine de la sécurité nécessite d'identifier les risques auxquels l'organisation est exposée. Il est essentiel d'acquérir avant tout la connaissance sur les groupes de cybercriminalité organisée : comprendre quelles sont leurs motivations et leurs modes opératoires. Ensuite utiliser cette connaissance pour mettre en place les moyens de détection et de protection adéquats. Ce type de services porte le nom d'*Advanced Threats Intelligence Service*.

Détecter

Les modes opératoires des attaquants sont de plus en plus sophistiqués : ils combinent de multiples méthodes et techniques pour atteindre leurs objectifs (qui peuvent être le vol de données, l'effacement, la perturbation ou l'arrêt de services). La combinaison de différentes méthodes et techniques rend les solutions traditionnelles, qui traitent unitairement chaque domaine, inefficaces.

La réponse à ce défi est l'intégration, voire l'interactivité, entre différentes solutions de sécurité, avec une approche holistique de monitoring de la sécurité de l'entreprise intégrée, basée sur la solution *Security Information and Events Management* (SIEM), la solution SIEM d'IBM étant IBM QRadar®.

La technologie IBM QRadar® est une solution analytique capable de passer au crible d'immenses quantités de données – à la fois internes et externes à l'entreprise – afin de découvrir des liens cachés, de détecter des modèles d'attaque, d'éradiquer des menaces existantes et de se préparer aux nouvelles.

Elle permet d'aller au-delà du traditionnel enregistrement des logs et d'évoluer vers un système complet pouvant absorber des montagnes de données et appliquer des méthodes d'analyse comportementale, afin de déterminer le moment précis où une violation pourrait se produire ou si elle est déjà en cours. De plus, cette technologie bénéficie de l'apport de X-Force® (laboratoire de recherche d'IBM), avec une mise à jour en temps réel des informations sur les vulnérabilités détectées, les adresses IP corrompues et les noms de domaine malveillants.

Gérer et remédier

Se doter d'une solution SIEM, combinée à la « *security intelligence* » – qui donne des renseignements sur les attaques sophistiquées potentielles –, est un prérequis pour développer les capacités de détection et de réaction face aux incidents de sécurité. Cependant, l'élément central est l'organisation en charge de la surveillance de la sécurité de l'entreprise. Cette organisation doit à la fois assurer les fonctions d'ingénierie de la solution SIEM, de surveillance des alertes, l'analyse de celles-ci et l'élaboration de plans d'actions, mais aussi de veille et d'analyse avancée (*forensics*). Elle doit également élaborer et produire les rapports opérationnels sur la sécurité à destination de la direction. Certaines de ses fonctions peuvent être confiées à un partenaire externe pour bénéficier de son expertise dans les attaques et donc d'une capacité d'analyse technologique rapide et pertinente.

Le point névralgique de l'organisation du centre de sécurité opérationnel est le dispositif de réponse en cas d'attaque : le *Computing Emergency Response Team* (CERT). Ce dispositif doit s'appuyer sur un processus de gestion de crise préalablement établi qui va identifier l'ensemble des acteurs à impliquer en cas d'attaque de sécurité et définir leurs responsabilités respectives. Il faut lui associer des compétences pointues en sécurité qui analysent la situation, aident à la prise de décision et effectuent les investigations (*forensics*) nécessaires, et ce pour mettre en place des mesures permettant à l'entreprise de se prémunir de ce type d'attaques dans l'avenir. Compte tenu de la rareté de ce type de ressources, il existe sur le marché des offres de type *Emergency Response Service* (ERS), qui permettent de faire appel à ces compétences en cas de nécessité.

Protection des données critiques

La gestion des risques informatiques traite in fine deux problématiques : d'une part, la perte ou la dégradation du service, d'autre part, le vol ou l'altération de données (y compris en cas de fraude), d'où l'importance de la protection des données sensibles. D'ailleurs, les nouvelles approches de sécurité qui abandonnent le paradigme de la protection périmétrique se basent sur le modèle centré sur les données.

Les programmes de protection des données critiques proposent une approche itérative multiétape outillée : définir, découvrir et comparer, sécuriser et surveiller. Cela pour un cycle de vie complet en matière de sécurité des données afin de protéger la rentabilité, la position concurrentielle et la réputation.

Définir

La classification des données est une tâche fastidieuse qui nécessite une forte implication du métier. Les acteurs de la sécurité ont développé une taxonomie (catégorisation de données) en fonction du secteur d'activité. Cette taxonomie constitue une base pour l'exercice de classification et permet d'accélérer le processus.

Découvrir et comparer

La localisation des données sensibles à la fois structurées et non structurées est un réel enjeu : le système d'information étant en perpétuelle évolution, la donnée se diffuse très facilement et sans réelle maîtrise. D'où la nécessité de s'appuyer sur les outils

qui permettent de localiser de façon dynamique ces données. Il existe des solutions pour localiser les données structurées (IBM Guardium®) et les données non structurées (par exemple, les outils développés par IBM Research combinant la technologie IBM StoredIQ® et IBM SPSS®).

Sécuriser et surveiller

Une fois que l'organisation a bien compris la nature et la criticité de ces actifs vitaux que sont les données et qu'elle est en capacité de les localiser, elle peut définir et mettre en place les moyens de protection adéquats en fonction de la classification effectuée. Les moyens de protection sont, entre autres, le chiffrement, la gestion des accès à ces données et la surveillance de l'ensemble des opérations effectuées sur ces données, sachant que les technologies de chiffrement sont intégrées par défaut à de nombreux *middlewares* du marché. Pour la surveillance des accès et des manipulations, on trouve, d'une part, les solutions spécialisées telles que IBM Guardium® pour les données structurées et, d'autre part, les solutions *Data Leakage Prevention* (DLP) d'éditeurs comme Symantec® ou Websense® pour les données non structurées.

Sécurité des applications

La transformation numérique incite l'entreprise à s'ouvrir de plus en plus vers l'extérieur et fait subir à son système d'information une évolution de plus en plus rapide avec la mise en place d'applications Web et mobiles.

Ces applications destinées aux employés, clients, partenaires constituent par ailleurs une surface d'exposition de l'entreprise aux risques externes. De plus, les exigences de flexibilité et de réactivité poussent les entreprises à développer et à mettre en production le plus rapidement possible. Dans ce contexte, il est nécessaire de trouver un équilibre entre la nécessité de sécuriser ses applications et les exigences du marché. Il suffit, dans ce cas, d'appliquer les règles de bon sens : préparer et former, tester et corriger, et, enfin, assurer le contrôle continu.

Préparer et former

Il s'agit d'abord d'établir les bonnes pratiques de développement pour chaque langage utilisé incluant les aspects de sécurité. Les professionnels dans ce domaine ont établi les règles à appliquer qui peuvent constituer un point de départ pour la définition des règles de développement spécifiques pour une entreprise. Ensuite, il est primordial de former les développeurs pour s'assurer que ces mesures sont respectées en appliquant la règle d'or dans ce domaine : la prise en compte de la sécurité dès la conception.

Développer, tester et corriger

Les technologies actuelles offrent des possibilités très intéressantes, et notamment la solution Arxan®, qui permet d'ajouter des éléments de sécurisation dans le processus de développement des applications mobiles. Ces éléments de sécurisation peuvent être le contrôle de l'état du mobile, le contrôle d'accès ou la prévention des tentatives d'insertion du code malicieux, etc.

Toutes ces mesures sont d'autant plus importantes que les entreprises ne maîtrisent plus le terminal sur lequel les applications sont installées : ce sont les tablettes et les smartphones des employés, des clients ou des partenaires.

Quant aux applications Web, il est essentiel de tester le code développé avant la mise en production et le plus tôt possible dans le processus de développement. Pour ce faire, il existe des solutions, tel IBM AppScan®, pour effectuer des tests de sécurité sur les applications en mode intrusif (en boîte blanche) ou en mode non intrusif (en boîte noire). Le fonctionnement de la solution consiste à détecter les vulnérabilités du code applicatif et de proposer les corrections. Ces solutions sont également disponibles en mode *cloud*, où les utilisateurs peuvent bénéficier du conseil des experts en la matière.

Assurer le contrôle continu

Les applications qui ont passé les tests de sécurité et ont été mises en production « subissent » continuellement les modifications pour répondre aux évolutions des besoins métiers. Ces modifications peuvent créer des failles dans l'application. Il est donc primordial de continuer à tester les applications en production pour s'assurer que ces évolutions n'ont pas ouvert une brèche aux attaquants. La fréquence de ces tests dépend bien sûr du rythme de mise en production des évolutions applicatives.

Ces tests nécessitent une industrialisation de la fonction avec la mise en place de l'outil de test au sein de l'entreprise ou bien son utilisation à partir du *cloud* (ce sont notamment deux options possibles de la solution IBM Appscan®).

Protection anti-DDoS

Pour finir, il faut mentionner les risques liés aux attaques de type « déni de services distribué » (DDoS). Ce sont les attaques les plus fréquentes et les plus faciles à réaliser. Nous assistons également à l'augmentation de la sophistication des attaques qui s'opèrent désormais aussi au niveau applicatif. Par conséquent, les entreprises doivent mettre en place des solutions de protection qui adressent ces deux aspects. Pour ce faire, elles ont à leur disposition deux types d'approche : les solutions qui peuvent être mises en place dans les *data centers* de l'entreprise ou bien celles qui sont fournies à partir du *cloud* d'un fournisseur. Il est indispensable que chaque entreprise développe sa propre stratégie de protection contre les attaques de type DDoS en tenant compte des risques et de son environnement technologiques.

En résumé, dans un contexte d'augmentation des menaces, de nombreuses entreprises investissent en ajoutant toujours plus d'outils à leur arsenal de sécurité informatique. Mais le foisonnement d'outils entrave la capacité de faire face aux enjeux de la sécurité des systèmes d'information, puisque aucun de ces systèmes ne communique de manière intelligible et transversale.

Il est donc indispensable de créer un réel programme de sécurité au sein de l'entreprise qui permettra de donner une vision d'ensemble concernant la posture de sécurité à adopter, de mettre en évidence l'interdépendance entre les différents domaines de sécurité et d'identifier les priorités et les projets qui en découlent.

Notes

1. IBM, le logo IBM, ibm.com *sont des marques appartenant à International Business Machines Corporation déposées dans de nombreux pays du monde entier. Les autres noms de sociétés, de produits et de services peuvent appartenir à IBM ou à des tiers. Les autres noms de sociétés, de produits et de services peuvent être les marques ou marques de services de tiers. La liste des marques IBM est disponible sur Internet à l'adresse* http://www.ibm.com/legal/copytrade.shtml.

*2. Étude de benchmark "*2014 Cost of Data Breach Study: Global Analysis*" sponsorisée par IBM et conduite par Ponemon Institute LLC, mai 2014 :* http://ibm.co/1mMGZJH

3. Étude "Understanding the Economics of IT Risk and Reputation" *sponsorisée par IBM et conduite par le Ponemon Institute® :* http://ibm.co/1FLnz2O

Pour une cybersécurité maîtrisée

Général (2S) Xavier de Marnhac

Senior Adviser, Lysios Public Affairs

Ancien directeur des opérations de la DGSE

Général (2S) Yves Mathian

Président, Clavys SAS

Ancien directeur technique de la DGSE

Chacun reconnaît que notre dépendance à l'informatique croît fortement et de façon continue. Des secteurs d'activité entiers génèrent des quantités gigantesques de données qu'il faut gérer et stocker avec la garantie de protection de leur intégrité et de leur confidentialité. Les entreprises ont récemment réalisé que, dans le cyberespace, il y a toujours un agresseur contre lequel il faut se protéger. Comment mettre en place le bouclier indispensable ? De multiples solutions existent. Mais, pour être pragmatique et rattraper notre retard en France, qui est réel en la matière, c'est sous l'angle de la souveraineté et de la convivialité dans les usages qu'il convient d'aborder la question.

Les révélations de WikiLeaks ou de l'affaire Snowden constituent la partie visible et spectaculaire du phénomène. Mais les attaques par saturation, intrusion ou déni de service, le vol de données d'identification et de mots de passe associés, les cas récents d'arnaque au président dont plusieurs entreprises ont été les victimes, ou enfin la fuite de données orchestrée pour nuire à l'image de l'entreprise, avec les conséquences financières lourdes qui en découlent, constituent autant d'exemples d'attaques cybernétiques caractérisées, cette forme moderne de « lutte du glaive contre le bouclier ».

Comme aux États-Unis, les menaces contre les réseaux informatiques sont « globalement en hausse » en Europe. C'est le constat que vient de dresser le directeur de l'Agence européenne chargée de la sécurité des réseaux et de l'information (Enisa [1], Udo Helmbrecht, en présentant la cartographie des risques pour les infrastructures Internet que l'organisme vient de publier [2]. Hackers, espions, employés

incompétents ou cyberterroristes... toutes les menaces pesant sur les réseaux européens sont recensées dans cette publication et illustrées sous forme de cartes et de tableaux. Et l'Enisa confirme au niveau européen les tendances enregistrées en 2013 : détournements d'adresse IP, *malwares* (3) et virus, espionnage, etc., représentent les formes d'attaque en nette progression.

Notre dépendance à l'informatique augmente exponentiellement depuis plusieurs décennies. Des secteurs d'activité entiers (transports ferroviaire, aérien et routier, médecine, banques, centrales nucléaires, pour ne citer que quelques exemples) et tous les systèmes industriels de contrôle et de supervision des réseaux informatiques et de télécommunications, évoqués par les spécialistes sous l'appellation de Scada (4), génèrent une quantité également exponentielle de données qu'il faut stocker, gérer, exploiter avec la garantie de protection de leur intégrité et de leur confidentialité. Aujourd'hui on nous parle de « *big data* », et demain, on nous parlera de « *smart cities* » !

Sur le plan institutionnel, la France s'est mobilisée (5) en se dotant d'outils, et notamment de l'Agence nationale de sécurité des systèmes d'information (Anssi), mais aussi d'une législation adaptée. L'identification d'opérateurs d'importance vitale (OIV) au sein des secteurs sensibles cités ci-dessus procède de la volonté de sécuriser les infrastructures indispensables au fonctionnement normal de nos sociétés industrialisées.

Pour les particuliers et les entreprises, ainsi que pour nos PME-PMI qui forment le cœur de l'économie française, la donne reste sensiblement différente. Sécuriser les communications et les échanges, protéger le patrimoine matériel et immatériel, conserver la confidentialité des négociations commerciales constituent autant d'enjeux, parmi d'autres, qui doivent être pris en compte. Nature et qualité des infrastructures informatiques, contrôle des logiciels et des services informatiques, pragmatisme des procédures et de la formation du personnel sont autant de défis qu'il est urgent de relever.

L'opinion publique en général, et le monde de l'entreprise en particulier, a récemment réalisé que dans cet univers où il y aura toujours un agresseur, quelle qu'en soit la nature, il devient indispensable de développer un bouclier qui assure un maximum de garanties tout en restant simple dans sa mise en œuvre. De multiples solutions existent, et il s'en invente tous les jours, mais elles se révèlent souvent dépendantes de l'étranger dans leur conception et complexes dans leur emploi. La combinaison de ces deux facteurs contribue à réduire de manière importante, voire radicale, leur efficacité.

Les enjeux de la cybersécurité sont nombreux et multiformes, mais c'est tout particulièrement en termes de souveraineté et de convivialité qu'il convient de les aborder.

Souveraineté

Dans le domaine de la sécurité informatique comme dans beaucoup d'autres, la souveraineté peut se définir comme la capacité de disposer de solutions nationales maîtrisées. C'est la garantie que des intervenants extérieurs (États en quête d'« intelligence », au sens anglo-saxon du terme, concurrents économiques, groupes de cybercriminels, hackers divers et variés, mouvements radicaux religieux, environnementalistes, pacifistes, syndicalistes, terroristes, etc.) verront leurs activités de pénétration ou de neutralisation rendues plus difficiles, voire impossibles, à la manière dont on procéderait pour rendre plus complexe la tentative d'effraction du voleur en multipliant les obstacles, en allongeant les délais de son action et en augmentant sa prise de risque. Pour revenir à des fondamentaux et au simple bon sens, quel homme raisonnable aurait comme idée pour protéger sa maison de confier ses clés au cambrioleur ?

Quelle est donc la réalité nationale aujourd'hui ? Qu'il s'agisse du cadre institutionnel public (Administration) ou encore du domaine privé (entreprises, particuliers), la situation n'est objectivement

pas brillante. Sans trop entrer dans les détails, on peut dire que, depuis l'échec du plan Calcul dans les années 1970 et le tournant raté de la micro-informatique des années 1980, la France a également manqué au début des années 2000 le virage de la protection de l'information.

Avant les années 2000, la sécurisation de l'information (pour faire simple, la cryptologie), relevait de la défense et de la sphère des matériels de guerre, dont l'usage et la commercialisation étaient très strictement contrôlés par l'État dans le cadre de sa fonction régalienne. L'État, ses services et ses industriels de défense concentraient le savoir-faire dans ce domaine.

À partir des années 2000, sous l'effet conjoint du développement généralisé du commerce électronique et de la libéralisation de la réglementation dans le domaine cryptologique, en Europe et dans le monde occidental, et en l'absence de politique industrielle soutenant l'émergence de sociétés françaises sur le marché de la sécurité, la France s'est mise dans une situation difficile.

Déjà hors-jeu en matière de fabrication de micro-ordinateurs et de systèmes d'exploitation avec l'arrivée massive de l'américain Microsoft, elle a laissé s'engouffrer et se généraliser des solutions étrangères, principalement anglo-saxonnes, parfois israéliennes ou sud-africaines (voire maintenant russes ou chinoises, et probablement bientôt indiennes !), jusqu'au cœur de l'Administration et dans quasiment toutes nos entreprises, quelle qu'en soit la taille. En matière de logiciels, l'intégrité des produits reste souvent difficile à évaluer, et l'existence avérée de *backdoors* (« portes dérobées ») dans bien des cas pose un défi aux outils de sécurité déployés par ailleurs.

Cette offensive étrangère s'est imposée dans tous les compartiments du jeu, du secteur des logiciels (systèmes d'exploitation, suites logicielles, antivirus, systèmes de supervision, de contrôle et de filtrage des flux Internet, etc.) à celui des équipements (micro-ordinateurs, smartphones, serveurs, routeurs). La France a perdu du terrain y compris dans le domaine des télécommunications, où elle avait pourtant acquis une place d'excellence avec quelques champions dont certains ont « changé de camp ».

Certes, le positionnement des industriels de la défense dans les domaines régaliens s'est maintenu, mais cette situation quasi monopolistique a de facto quasiment interdit toute percée significative de PME dans ce créneau. Leur offre, essentiellement tournée, historiquement et culturellement, vers le secteur de la défense et les besoins militaires, se montre rarement adaptée aux attentes et aux moyens du secteur privé, en particulier celui des PME-PMI.

Par ailleurs, l'obsolescence très rapide des technologies informatiques et de communication contemporaines, devenue une constante depuis leur éclosion il y a cinquante ans – et qui se mesure à quelques mois aujourd'hui dans certains domaines –, s'accommode mal des réponses souvent laborieuses de la mécanique compliquée et lente des programmes d'armement telle que les industriels de la défense la pratiquent.

Cette obsolescence rapide touche directement les clients et les usagers. En effet, les petites entreprises (TPE-PME), dont le bon fonctionnement de l'organisation dépend du système informatique et des flux de données (messagerie, gestion de base de données, serveurs, sites Web, suites bureautiques, etc.), sont devenues plus vulnérables à cette obsolescence car elles ne disposent pas forcément d'une direction informatique, encore moins d'un RSSI (6), ou d'un prestataire en sécurité informatique.

Un logiciel ou un système d'exploitation obsolètes ne seront pas compatibles avec les produits récents intégrant de nouveaux protocoles ou de nouvelles technologies. À terme, la mise en œuvre de solutions qui ne sont plus à jour pourra fortement handicaper le fonctionnement de la société et l'exposera à des failles de sécurité. Comment faire face ?

Confrontées à la faiblesse de l'offre française, incapables de suivre le rythme effréné du développement dans ce secteur, les entreprises se tournent aujourd'hui

« naturellement » vers des solutions étrangères, souvent *low cost*, sacrifiant la sécurité et l'intégrité des données à la sûreté de fonctionnement des systèmes et des réseaux informatiques.

Plus largement, dans le domaine du stockage et de la sécurisation des données, le développement d'offres de *cloud* (« stockage en nuage »), le plus souvent de conception étrangère, généralement associées à une politique d'externalisation, pose de sérieuses questions de garantie de la protection de ces données. Ces offres de *cloud*, extrêmement attractives et bon marché, permettent aux entreprises, en particulier les petites, de se concentrer sur leur « cœur de métier ». Elles réalisent du même coup des économies substantielles en personnel et en moyens dans le domaine de la maintenance de leurs systèmes d'information.

Dans sa tentative de créer une offre de *cloud* souverain – jugée indispensable en particulier par l'Administration –, la France, avec un certain nombre de ses « majors » industriels, patauge depuis plusieurs années (7). Au moment où le pays a compris l'importance de protéger ses organismes d'importance vitale contre des agressions extérieures, l'externalisation des données sensibles pour des raisons essentiellement économiques devient pour le moins paradoxale. Dans le cadre de l'application des futures directives attachées à la protection des OIV, l'État aura-t-il alors le poids suffisant pour contraindre les entreprises ayant opté pour des solutions étrangères à un retour en arrière qui s'avérera aussi complexe que coûteux ?

Sans une volonté politique affirmée et une mobilisation industrielle forte, ces quinze ans de retard seront difficiles à rattraper. Et, dans tous les cas, cela prendra du temps et exigera beaucoup de ressources.

Convivialité

Parce qu'elle apparaît comme un facteur essentiel de l'adhésion des utilisateurs au déploiement de la cybersécurité, la convivialité peut se définir comme la résultante de l'ergonomie et de la simplicité des procédures. Sans oublier qu'aujourd'hui les critères de coûts et d'ergonomie sont prépondérants dans le choix d'un système et prennent le pas, bien souvent, sur l'argument de la sécurité proprement dite.

À l'heure où la frontière entre vie professionnelle et vie privée s'efface, le dirigeant d'une entreprise, que celle-ci soit cotée au CAC 40 ou une simple PME, ne veut pas se compliquer la vie. Il veut disposer d'un seul terminal (nomade ou pas) qui lui permette, d'une façon simple, de basculer d'un besoin ordinaire à une réponse sécurisée. Ce qui est vrai pour le dirigeant s'applique à tous les acteurs. L'expérience prouve que la multiplication des contraintes de mise en œuvre se traduit le plus souvent par une augmentation de la prise de risque par refus d'utilisation. La meilleure solution de sécurité, si elle n'est pas utilisée, ne sert à rien. Ce qui replace l'individu au cœur du système.

C'est pourquoi les outils destinés à des interlocuteurs finaux dans une approche B2C (8) doivent tenir compte, dès leur conception, des attentes des clients, principalement en matière de convivialité et d'ergonomie. Le développement des systèmes doit également intégrer, dès la conception, les procédures adaptées avec le souci permanent de la simplicité d'installation.

En effet, à côté de la convivialité qu'on peut qualifier de « technique », qui relève de la conception des outils, il ne faut pas sous-estimer l'importance d'une convivialité de « procédure », dont le pragmatisme et la simplicité doivent assurer la complémentarité avec celle fournie par la technique pour obtenir l'optimisation finale recherchée. Elle suppose non seulement l'existence de telles procédures, mais aussi la formation du personnel chargé de les déployer ainsi que le contrôle effectif du respect de celles-ci. Car, bien souvent, comme dans les accidents d'avion, c'est le facteur humain qui reste la principale cause de vulnérabilité. À quoi bon protéger son ordinateur quand on l'« oublie » sur son siège dans le Thalys, entre Paris et Bruxelles, le temps d'aller boire un verre au wagon-bar ?

Dans le domaine des risques informatiques, l'angélisme le dispute à la naïveté chez beaucoup d'acteurs, qu'ils appartiennent aux grands groupes ou au monde des PME-PMI.

Bien souvent, les entreprises de toute taille et leurs dirigeants ne se préoccupent de la sécurité de leurs informations que lorsque le sinistre est là, que la fuite ennuyeuse est sortie dans la presse. Avec ce sentiment diffus mais bien réel qu'on ne traite pas d'information véritablement sensible (sur le thème : « nous sommes des gens matures et nous ne disons rien d'important au téléphone ou par mail »). Les mêmes qui s'insurgeaient en 1988, lorsque le journaliste écossais Duncan Campbell dévoilait l'existence du programme Echelon, et aujourd'hui, vingt-cinq ans après, poussent des cris d'orfraie face aux atteintes à la vie privée révélées par l'affaire Snowden sont ceux qui envoient sur Internet leurs informations confidentielles par mail « en clair » (parfois depuis leur domicile à partir de la « box » familiale…) ou qui étalent leur vie privée sur Facebook. Ce sont les mêmes qui s'étonnent ensuite d'avoir raté tel appel d'offres ou d'avoir perdu tel marché à l'export, se plaignant parfois même de ne pas avoir été suffisamment accompagnés par l'État dans leurs ambitions à l'international !

Le temps perdu ne se rattrape pas. Il ne sert à rien de se lamenter sur les échecs passés. Au contraire, il faut affronter résolument les risques du temps présent et se préparer à ceux de demain. À court terme, la nécessaire souveraineté, en particulier dans le *cloud*, demeure un impératif vers lequel il faut tendre en recourant aux solutions qui existent, même dégradées dans ce domaine. Les grands industriels et opérateurs du secteur peuvent y pourvoir. Un dialogue étroit doit se poursuivre entre utilisateurs et fournisseurs de solutions avec le souci permanent de la convivialité et de la simplicité des outils comme des procédures. C'est le gage d'une sécurité accrue.

À moyen terme, il convient de restaurer une capacité souveraine. Fédérer les PME et les laboratoires du secteur s'impose afin de leur permettre de répondre à des appels d'offres et de satisfaire les besoins de PME-PMI clientes, qui restent les grandes oubliées en matière de cybersécurité. Des initiatives ont déjà été prises comme en 2014 celle d'Hexatrust, groupement associatif de PME expertes dans le domaine de la sécurité de l'information.

Il conviendra également de dynamiser le tissu industriel de la cybersécurité. Mais cela en évitant, comme trop souvent, une absorption ou une dilution pure et simple, au sein de plus grands groupes, de PME porteuses de solutions pertinentes mais en difficulté financière, ce qui entrave toute capacité d'innovation et de réactivité dont sont pourtant capables les PME du secteur.

Enfin, il faudra créer les conditions qui permettent à des PME innovantes du secteur de la cybersécurité de se développer. Cela veut dire les faire émerger sur le marché national et à l'exportation sans les contraindre par des barrières administratives de certification ou de contrôle d'export aussi peu lisibles que coûteuses qui les disqualifient de facto face à la concurrence étrangère.

La France possède de réels atouts dans le domaine de la protection de l'information. Elle jouit d'une expertise reconnue au sein d'une Europe dans laquelle de nombreux pays ont eux-mêmes des faiblesses et des besoins. Ils n'attendent que d'être satisfaits par des solutions de confiance avec l'objectif de préserver la confidentialité de leurs données et de celles qu'ils échangent avec leurs partenaires européens. Suivant le bon adage qui veut que la « performance » d'une chaîne de valeur ne vaut que par celle de son maillon le plus faible, il serait bienvenu pour la nouvelle France industrielle d'avoir de l'ambition dans sa feuille de route. Il s'agirait sinon de rattraper le temps à jamais perdu, du moins de combler en priorité les trous dans la raquette en valorisant l'offre française en cybersécurité sur le marché européen et à l'international.

Notes

1. Enisa : European Network Information Security Agency.

2. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure/iitl

3. Malware : *« logiciel malveillant ».*

4. Scada : supervisory control and data acquisition.

5. Voir le dernier Livre blanc sur la défense et la sécurité nationale daté de 2013. Disponible en PDF : http://www.livreblancdefenseetsecurite.gouv.fr

6. RSSI : responsable de la sécurité des systèmes d'information.

7. Voir au sujet de l'échec du « cloud *souverain » :* http://itsocial.fr/actualites/fournisseurs/orange-rachete-cloudwatt-lechec-du-cloud-souverain

8. B2C : Business to Customer. *Activités tournées vers le consommateur (à opposer à B2B :* Business to Business*).*

Le canari dans la mine de charbon

Frédérick Douzet

Professeure à l'Institut français de géopolitique, Université Paris-8

Titulaire de la chaire Castex de cyberstratégie

à l'Institut des hautes études de défense nationale

Les cyberattaques contre Sony Pictures fin 2014 sont emblématiques des nouveaux risques auxquels sont confrontées les entreprises en raison de leur dépendance accrue aux systèmes d'information et de communication interconnectés à l'échelle planétaire. L'affaire Sony Pictures comprend tous les ingrédients d'un cocktail toxique pour une entreprise : vol et perte de données, divulgation publique de données personnelles et d'informations confidentielles, atteinte à la réputation de l'entreprise, atteinte à sa capacité de mener à bien ses activités. Mais elle dépasse aussi largement le cadre de l'entreprise, illustrant l'extrême intrication des enjeux économiques, politiques, juridiques et sécuritaires dans le cyberespace. Elle démontre que le cyber-risque n'est pas juste un problème technique mais qu'il doit faire l'objet d'une stratégie de management au plus haut niveau de l'entreprise.

Un risque complexe et protéiforme

Caractéristiques et montée en puissance des cyberattaques

Le développement massif du numérique révolutionne nos méthodes de travail comme nos modes de vie et constitue une source de croissance essentielle dans une économie globalisée. Mais l'interconnexion des systèmes d'information et l'explosion des services en ligne engendrent aussi de nouveaux risques. En l'espace de quelques années, les incidents sur les systèmes d'information se sont multipliés, et les rapports d'expertise se font de plus en plus alarmistes sur l'ampleur et l'impact des attaques contre les entreprises, alors que de nouveaux modes d'action et de nouvelles vulnérabilités ne cessent d'apparaître.

En mars 2013, dans un retentissement médiatique sans précédent, le rapport de la société Mandiant [Mandiant, 2013] a dénoncé le vol de centaines de térabytes de données dans près de 141 entreprises du secteur industriel victimes d'intrusions chinoises. Les actes malveillants les plus sérieux via les réseaux informatiques incluent principalement l'espionnage, le sabotage, le vandalisme et le vol de données.

Les conséquences peuvent être désastreuses. En 2012, l'entreprise d'hydrocarbures Saudi Aramco

a dû mettre au rebut 30 000 ordinateurs endommagés d'un coup par une cyberattaque. Les actions récentes contre les installations industrielles font craindre pour la sécurité des infrastructures vitales. En février 2013, en une nuit, un vaste réseau de cybercriminels a réussi à dérober plus de 40 millions de dollars à diverses banques internationales. En 2015, les premiers chiffres internes de Sony Pictures estiment les dégâts à près de 35 millions de dollars, et la vice-présidente a été contrainte de démissionner après la divulgation de courriers électroniques jugés racistes.

Les défis pour gérer ces risques sont multiples. La technologie évolue très vite, ce qui nécessite une analyse constante de la menace et une très grande réactivité. L'architecture et la protection des systèmes d'information de la cible sont tout aussi importantes que les compétences de l'assaillant pour déterminer le succès d'une attaque. La multiplication des objets connectés à double usage personnel et professionnel complique la gestion de la sécurité pour les entreprises.

Outre les attaques opportunistes relativement basiques qui changent de cible lorsqu'elles rencontrent des résistances, on compte de plus en plus d'attaques ciblées et sophistiquées visant précisément une entreprise ou une organisation, qui sont les plus difficiles à anticiper et à contrer. Lorsqu'un adversaire est déterminé à pénétrer un système et y consacre tous les moyens nécessaires, il a de fortes chances d'y parvenir s'il dispose des ressources adéquates.

Les mesures de protection des systèmes d'information sont indispensables mais ne peuvent garantir la sécurité absolue. Une part de risque persistera nécessairement, en raison de la probabilité croissante d'attaques de grande ampleur toujours plus innovantes, ciblées et sophistiquées, alors que la « surface d'attaque » des entreprises toujours plus interconnectées, au patrimoine de plus en plus dématérialisé, ne cesse de s'étendre. Le retentissement planétaire de l'attaque contre Sony Pictures montre les proportions que peuvent prendre ces actes malveillants, leurs conséquences sur l'entreprise ainsi que l'importance du contexte géopolitique.

Une difficile appréhension pour l'entreprise

Le succès des hackers a révélé la vulnérabilité – voire l'impréparation – de Sony Pictures face aux cybermenaces et les manquements effarants à quelques règles de sécurité de base de la part d'un grand groupe pourtant déjà victime d'intrusions par le passé et dont la valeur repose largement sur son patrimoine immatériel. Peu de données étaient sécurisées par mot de passe, et les experts ont retrouvé dans les ordinateurs des fichiers entiers d'identifiants et de mots de passe. Les données sensibles n'étaient pas séparées des autres, et peu d'entre elles étaient chiffrées (salaires, numéros de Sécurité sociale). Sony Pictures n'utilisait par ailleurs pas de processus de double authentification. Cela dit, le FBI estime que 90 % des entreprises seraient tombées face à une telle attaque.

La prise de conscience de la part des dirigeants d'entreprise n'est pas toujours à la hauteur des enjeux, même si de grands progrès ont été faits au cours de ces dernières années. Il faut dire que le risque est particulièrement complexe à appréhender et plus encore à quantifier. On mesure généralement le risque à l'aune de l'impact d'un incident sur les activités et les objectifs d'une entreprise. Encore faut-il que les entreprises sachent qu'elles ont été attaquées. Le délai moyen de détection d'une attaque en France est aujourd'hui d'environ 400 jours ; la société Mandiant l'estime à 356 jours pour les États-Unis. Contrairement au risque incendie, une entreprise peut ignorer un cyber-risque dont les conséquences ne se feront sentir qu'à moyen ou long terme. Sony Pictures n'a pris connaissance de l'intrusion dans ses systèmes qu'à partir du moment où les hackers ont émis des revendications et commencé à diffuser publiquement des informations confidentielles.

Les coûts directs sont multiples et élevés, entre le nettoyage et la remise en état des systèmes d'information, les pertes de données et les pertes d'exploitation, le vol de données (propriété intellectuelle, secrets d'affaire, données financières, etc.), l'atteinte à l'image,

les frais de gestion de crise ou encore la notification et l'indemnisation des personnels. L'enjeu de la responsabilité juridique de l'entreprise est par exemple directement posé par les personnels de Sony Pictures, qui ont lancé des *class actions*. Or, ces coûts sont difficiles à évaluer, d'une part parce qu'on manque de statistiques concernant un grand nombre d'entreprises, celles-ci se montrant très réticentes à divulguer les attaques subies pour protéger leur réputation et leurs intérêts, et d'autre part parce qu'il n'existe pas de méthode de calcul standardisée qui fasse l'objet d'un consensus. La notion de retour sur investissement est donc difficilement chiffrable, ce qui incite à considérer les dépenses de sécurité comme des pertes sèches et donc à les limiter.

Enfin, l'existence de menaces et de vulnérabilités ne signifie pas qu'elles seront exploitées et que leur impact sera important. L'appréhension du risque nécessite donc de comprendre d'où vient la menace et d'avoir une vision globale de l'entreprise dans son environnement économique et géopolitique.

Une très forte intrication des enjeux

L'affaire Sony dépasse largement le cadre de l'entreprise et illustre ainsi la très forte intrication des enjeux économiques, politiques, juridiques et sécuritaires dans le cyberespace. Cet acte qualifié de cybercriminel, voire de vandalisme, s'inscrit dans des rivalités géopolitiques internationales, sur fond de menace terroriste, et a entraîné des mesures de rétorsion au plus haut niveau du pouvoir. Le secret qui entoure l'affaire incite à la plus grande prudence sur les faits et les protagonistes. Elle démontre toutefois qu'à l'heure des réseaux partagés il n'est pas toujours aisé de démêler ce qui relève de la cybercriminalité, de la compétition économique ou des rivalités de pouvoir entre puissances.

Les réseaux sont aussi un outil au service de la puissance des États, dont les plus avancés mènent des actions offensives dans le cyberespace en exploitant des vulnérabilités. Edward Snowden a révélé que les États-Unis avaient pénétré le réseau nord-coréen, fort probablement en passant par les réseaux chinois, avant même l'attaque contre Sony Pictures (1). Or, les tensions entre la Chine et les États-Unis sont vives sur les questions « cyber », à la suite de la mise en examen, en mai 2014, de cinq officiers de l'armée chinoise pour espionnage. Le gouvernement américain a désigné la Corée du Nord comme responsable des attaques contre Sony Pictures – sans toutefois révéler ses preuves à caractère sensible, malgré les doutes émis publiquement par de nombreux experts, ce qui rend l'affirmation invérifiable – et a menacé le pays de représailles dont certaines seraient visibles et d'autres non. Le blocage du réseau nord-coréen apparaît ainsi comme une probable contre-mesure – non revendiquée – du gouvernement américain, ou comme l'opportunité d'un test grandeur nature de ses capacités. À moins que l'attaque contre Sony Pictures ne soit la contre-mesure d'actions offensives menées par le gouvernement américain, ou un acte crapuleux opportunément déguisé en combat politique, voire tout autre chose.

Les cybercapacités des États relèvent d'une question de souveraineté si sensible qu'elles font l'objet de plus de secrets encore que le nucléaire, ce qui limite fortement la coopération internationale dans la lutte contre la cybercriminalité. Cela explique en partie le risque et les difficultés à se protéger, alors même que les enjeux du secteur privé rejoignent ceux des gouvernements. Le vol de propriété intellectuelle et de technologie en proportions industrielles affecte la puissance économique des nations, et la vulnérabilité des infrastructures vitales – dont beaucoup sont gérées par le secteur privé – préoccupe au plus haut point les gouvernements. Pour autant, le risque est avant tout assumé par les entreprises et il est incontournable.

Le cyber-risque doit ainsi se comprendre dans un contexte géopolitique plus global et faire l'objet d'une véritable stratégie de management de la part des entreprises. Ce n'était vraisemblablement pas le cas de Sony Pictures, de l'aveu même de son directeur : « Nous sommes comme le canari dans la mine de

charbon, ça c'est sûr. Il n'y a pas de manuel pour ça, vous naviguez essentiellement à vue et prenez des décisions sans pouvoir vous référer à beaucoup d'expériences passées, ni les vôtres ni celles des autres. C'est un terrain complètement nouveau. (2) »

De la nécessité d'une cyberstratégie

Le cyber-risque n'est donc pas une simple question technique, bien qu'il soit souvent considéré comme le problème des informaticiens et laissé aux mains des responsables de la sécurité des systèmes d'information des entreprises. Il nécessite de sortir de l'approche en silo et d'instaurer un véritable dialogue entre les informaticiens, qui analysent le cyber-risque à l'aide de méthodes qui leur sont propres mais non partagées en dehors de leur communauté, et les risk managers, qui travaillent en liaison avec des sociétés d'assurance ou des courtiers. Ce dialogue n'est pas simple à mettre en place mais il est indispensable, parce que la sécurité absolue n'est ni possible ni même souhaitable.

D'une part, avec la prolifération des attaques, l'innovation technologique constante et la diversité croissante des menaces, il est illusoire de croire pouvoir protéger tout, de tout le monde. En 2012, le directeur du FBI, Robert Mueller, estimait qu'il arriverait un moment où aucune entreprise ne pourrait se vanter d'être protégée : « Il y a deux types d'entreprises, celles qui ont été hackées et celles qui le seront. (3) » Ou « celles qui ne le savent pas », disent aujourd'hui les experts en cybersécurité. D'autre part, la sécurité a un coût, pas seulement financier mais aussi relatif au confort d'utilisation des outils, à l'innovation, à la productivité, à la réactivité dans une économie qui fonctionne sur la mise en réseau et l'ouverture. Plus le système est verrouillé, plus les procédures sont lourdes et plus les performances de l'entreprise s'en ressentiront. Il est donc indispensable d'établir des priorités et des stratégies, ce qui est le rôle du management.

L'analyse de la menace comprend certes un volet technique, mais elle nécessite aussi de connaître ses ennemis, de savoir ce qui a de la valeur pour eux et doit être protégé en priorité. Au-delà de la simple concurrence économique, c'est aussi ce que représente l'entreprise symboliquement ou politiquement qui peut la conduire à devenir une cible. Le risque géopolitique comporte désormais une « cyberdimension » qu'il faut prendre en considération dans une approche globale.

L'élaboration d'une stratégie passe aussi par une bonne compréhension de son patrimoine matériel – pouvant être saboté par une attaque – et immatériel. Quelles sont les infrastructures à cloisonner ? Quelles données ont une valeur stratégique et doivent bénéficier du plus haut niveau de protection ? Pendant combien de temps ? Quelle est la part de risque que l'entreprise peut supporter ? Que l'on est prêt à accepter ?

Les moyens à mettre en œuvre pour protéger son patrimoine sont techniques mais aussi humains : bonnes pratiques, sensibilisation et formation du personnel. L'enjeu n'est pas seulement de prévenir ou contrer l'attaque, mais aussi d'en limiter l'impact. Cela nécessite de penser en termes d'architecture des réseaux et de procédures, mais aussi de favoriser la résilience afin d'assurer la continuité de l'activité et de prévoir la gestion de la crise qui ne manquera pas d'arriver. Une identification claire des acteurs et de leur rôle (au sein de l'entreprise et à l'extérieur), la mise en place de procédures, la pratique d'exercices d'entraînement peuvent faire gagner un temps précieux sous le feu de l'attaque.

Enfin, l'externalisation du risque résiduel permettrait de mieux intégrer le cyber-risque dans une analyse de risque globale. Mais l'offre de cyberassurance reste encore peu développée en France, même si des initiatives commencent à émerger.

Les entreprises ne peuvent guère lutter à leur niveau contre la prolifération des cyberattaques. La réduction de leur nombre relève plutôt de l'action des États, qui peuvent légiférer et collaborer afin de

mieux identifier, appréhender et traduire en justice les criminels, et établir des normes de comportement responsable dans le cyberespace. Les entreprises peuvent en revanche développer des stratégies de gestion du risque pour en limiter les conséquences. Cela nécessite un dialogue transversal interne complexe à mettre en œuvre au plus haut niveau du management de l'entreprise. Ce dialogue doit aussi se faire en partenariat avec les agences publiques en charge de la cybersécurité, voire au-delà entre entreprises d'un même secteur, même si le partage d'information reste très sensible en raison de l'utilisation des mêmes réseaux à des fins d'intelligence et d'espionnage par d'autres acteurs économiques ou politiques. Développer une véritable stratégie à l'égard du cyber-risque, c'est positionner ses forces et coordonner ses actions pour atteindre ses objectifs de croissance et maintenir un avantage compétitif pour l'entreprise. Cela implique de décider ce qui a valeur stratégique pour l'entreprise, quelle part de risque est acceptée, afin d'adapter ses actions en conséquence. C'est le rôle du comité exécutif de l'entreprise, qui, comme le démontre l'affaire Sony, doit s'impliquer dans la gestion de ce risque complexe mais inéluctable.

Notes

1. Citation traduite par l'auteur. Source : D. E. Sanger et M. Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say", Nytimes.com*, 18 janvier 2015.* http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

2. Citation traduite par l'auteur. Source : "Sony Pictures CEO on Hack: 'There's No Playbook for This'", Billboard.com*, 9 janvier 2015.* https://www.billboard.com/articles/news/6436362/sony-pictures-ceo-on-hack-theres-no-playbook-for-this

3. Citation traduite par l'auteur. Source : "FBI Director: Hacking Will Replace Terrorism As The Nation's Top Worry", Businessinsider.com*, 1er mars 2012.* http://www.businessinsider.com/robert-mueller-fbi-hacking-terrorism-2012-3?IR=T

Bibliographie

AGHROUM C. ; CALÉ S. (dir.), *Protection de l'information. Pourquoi et comment sensibiliser*, L'Harmattan, Paris, 2014.

DOUZET F. ; HÉON S., « L'analyse du risque cyber, emblématique d'un dialogue nécessaire », *Sécurité & Stratégie*, n° 14, novembre 2013.

Hérodote, « Cyberespace : enjeux géopolitiques », n° 152-153, 2014.

Mandiant, "APT1: Exposing One of China's Cyber Espionage Units", rapport, février 2013.

ROSS A. ; BARTON C. ; BÖHME R. ; CLAYTON R. ; EETEN M. J. G. (VAN) ; LEVI M. ; MOORE T. ; SAVAGE S., "Measuring the Cost of Cybercrime", Workshop on the Economics of Information and Security (WEIS), 2012. Disponible en PDF : http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Enjeux de l'assurance des cyber-risques

Clotilde Zucchi

Directeur marché français, International Financial Lines, XL Insurance

L'évolution des méthodes de travail des entreprises conduit celles-ci à disposer de nombreuses données dont l'exploitation et la protection sont au cœur de leur stratégie et indispensables à leur développement. Les assureurs accompagnent leurs clients dans la protection de leur actif intangible par des couvertures désormais bien établies, sur une base néanmoins singulière combinant des garanties dommages et responsabilité civile dont la mise en œuvre est différente. Les conséquences d'une intrusion informatique doivent également être appréhendées dans les études de risques réalisées au titre d'autres contrats d'assurance dont l'objet initial était autre. La gestion des cumuls de risques prend alors une dimension particulière. L'appréhension des cyber-risques nécessite d'inclure la prévention d'un risque systémique dont l'étendue reste à explorer.

Sur la base du double constat de l'évolution des méthodes de travail de toutes les industries humaines avec l'introduction de l'informatique et de la mise en œuvre des législations relatives à la protection des données personnelles et confidentielles (voir encadré p. 57), les assureurs ont entendu les demandes de leurs clients, entreprises commerciales, liées à leur besoin d'accompagnement dans la protection contre les risques engendrés par l'utilisation des données informatiques. En cas d'atteinte aux données détenues par une entreprise, il est vital pour cette dernière de pouvoir les reconstituer rapidement afin de poursuivre son activité, mais aussi de répondre de sa responsabilité à l'égard des personnes dont les données personnelles et/ou confidentielles ont été compromises.

La plus grande disponibilité des données, d'une part, et le fait que de nombreux acteurs économiques ou étatiques disposent de bases de données personnelles, d'autre part, ont conduit les législateurs à renforcer la protection de la vie privée. Ceux-ci ont été jusqu'à créer, notamment pour les banques et les fournisseurs de communications électroniques (Internet et téléphone), une responsabilité objective autour du maintien de l'intégrité de ces données.

L'utilité, voire quelquefois la nécessité, de transférer ces risques à des sociétés d'assurance repose sur le fait que les données sont un actif intangible de l'entreprise dont l'importance économique est grandissante. Le débat actuel sur l'appropriation du *big data* en est l'illustration parfaite et conditionne bon nombre de développements, voire la survie d'entreprises.

C'est pourquoi les assureurs ont considéré qu'ils devaient accompagner leurs clients avec un contrat unique comportant tant des garanties pour compte propre (assurance dommages, dans notre langage d'assureur) que des garanties de responsabilité. Par exception à ce qui se pratique habituellement sur nos marchés, les garanties offertes ne sont pas bâties autour de la nature du préjudice subi (dommage ou responsabilité) mais autour de l'objet même de leur préoccupation (la donnée personnelle et/ou confidentielle) afin d'appréhender l'ensemble des conséquences financières en cas de compromission d'un réseau d'information et d'une donnée.

Que couvre l'assurance cyber-responsabilité ?

Les données étant un actif intangible, il n'est pas aisé d'obtenir par la souscription de contrats classiques de responsabilité civile, exploitation ou professionnelle, ou de dommages aux biens une réponse appropriée aux multiples conséquences d'une atteinte aux réseaux d'information de l'entreprise ou aux données personnelles ou confidentielles qu'elle détient.

L'objectif des contrats dits de « cyber-responsabilité » étant de protéger l'entreprise contre l'ensemble des conséquences d'une atteinte aux données qu'elle détient et aux réseaux d'information sur la base desquels elle exerce son activité professionnelle, le choix a été fait d'intégrer à la fois des garanties de dommages qui protègent des sinistres survenant dans l'entreprise et des garanties de responsabilité civile en cas de mise en jeu de cette dernière par des tiers.

L'ensemble des offres des marchés d'assurance au niveau international se stabilise autour des garanties ci-après détaillées. Les assureurs se différencieront essentiellement par les montants de garantie, les sous-limites ou les franchises proposés, mais aussi par certains services de prévention ou d'accompagnement des assurés dans la gestion de la crise que nécessite toute atteinte à un système d'information ou à des données détenues.

Garanties dommages en péril dénommé

- Les frais de reconstitution des données dans la mesure où il existe une sauvegarde récente.

- Les frais supplémentaires d'exploitation. Il s'agit d'assumer des frais par nature exceptionnels et directement consécutifs à une atteinte au réseau d'information et permettant à l'entreprise de revenir dans l'état où elle se trouvait avant le sinistre : location de locaux ou de matériels supplémentaires, paiement d'heures supplémentaires, recours à la sous-traitance, etc.

- Les pertes d'exploitation, souvent définies comme la perte de marge brute consécutive au sinistre pendant une période déterminée. La franchise applicable à cette garantie est le plus souvent exprimée en heure d'indisponibilité des systèmes avec quelquefois un maximum exprimé en montant.

- Les frais de remédiation ou frais de l'informatique légale (*forensic*), *i.e.* les frais d'investigation respectant les techniques et protocoles de recueil des preuves d'une atteinte à un système d'information ou à des données permettant de qualifier les faits et de mettre en œuvre les moyens de remédiation. Cela peut inclure également, selon le contrat, les cas de suspicion d'attaque informatique.

- Les frais de notification auprès des autorités compétentes et/ou des personnes concernées, *i.e.* les coûts de rédaction de l'information et de la communication aussi étendue que nécessaire de l'existence d'une atteinte aux données précisant la nature des données compromises, les conséquences que cela implique pour les individus et les précautions à prendre, ainsi que les mesures prises par l'entreprise pour limiter les conséquences du piratage. La notification répond à un formalisme très précis déterminé par le règlement européen UE n° 611/2013 de la Commission du 24 juin 2013.

Cette garantie peut aussi être étendue aux frais de notification réalisés volontairement par l'entreprise en dehors de toute obligation légale.

• Les frais de gestion de crise, y compris la mise en place d'une assistance téléphonique.

• Les frais de relation publique à la suite d'un événement médiatique.

• Les frais de suivi d'une éventuelle usurpation d'identité à la suite d'une atteinte aux données. Les contrats sont cependant assez contraignants sur les conditions de prise en charge de ces frais.

• Une garantie extorsion dont l'objectif est double : la prise en charge des frais et honoraires des spécialistes informatiques chargés de vérifier la véracité de la menace et le paiement de rançon.

• Une garantie des pénalités PCI DSS (voir encadré p. 57), y compris les frais de l'expert habilité par le Conseil des normes PCI DSS chargé de qualifier l'existence et l'étendue de la violation des données de cartes bancaires. Cette garantie n'est cependant pas systématique pour l'ensemble des assureurs et ne peut intéresser que des sites marchands appliquant les normes PCI DSS.

• Les frais d'enquête et de sanction des autorités administratives dans la mesure où ces sanctions sont assurables. Cela dépendra de leur nature civile ou pénale et de l'État dans lequel elles sont prononcées.

Garanties de responsabilité civile

L'objet est de couvrir la responsabilité civile encourue par la société du fait d'une atteinte à des données personnelles ou confidentielles ainsi qu'à son système d'information ou à un système dont elle est responsable. Cela couvre également la responsabilité de l'entreprise du fait de ses sous-traitants. Certains assureurs ont bien intégré que nous sommes ici dans le cadre d'une responsabilité objective, *i.e.* sans faute, mais d'autres accordent leur garantie uniquement sur la base du triptyque traditionnel : faute, préjudice et lien de causalité. Cela aura des conséquences sur la charge de la preuve et l'application des garanties.

Il est à noter que ces deux natures de garantie ne répondent pas aux mêmes critères de déclenchement de la couverture. Dans le premier cas, il s'agira de la survenance d'un événement garanti, et, dans le second, de la réclamation d'un tiers. Cela contraint les assureurs, au regard du droit français des assurances, à soigneusement détailler le fonctionnement de la garantie et sa mise en jeu, notamment au titre des garanties subséquentes. Les contrats peuvent ainsi sembler complexes et peu faciles d'appropriation à des assurés peu familiers des techniques assurancielles. Le développement de ces solutions auprès d'entreprises de petite taille poussera certainement les assureurs à porter leurs efforts sur la qualité rédactionnelle des contrats et la pédagogie dans l'explication de ceux-ci.

L'assurance cyber-responsabilité : marché et enjeux

L'assurance des risques informatiques n'est pas aussi récente que le laisse penser l'actuelle médiatisation des enjeux de cybersécurité. Si les premiers contrats remontent aux années 1990, ceux dont le contenu a été exposé ci-dessus ne sont adaptés et régulièrement vendus en Europe, et notamment en France, que depuis 2010.

Vers l'uniformisation des motivations d'achat

L'évolution des législations du point de vue de l'obligation de notifier les atteintes aux données personnelles a été le facteur déterminant de l'augmentation du nombre de contrats, phénomène constaté d'abord aux États-Unis d'Amérique. Il est

néanmoins intéressant de relever que la motivation principale des assurés pour l'achat de ces garanties varie selon leur implantation géographique. En Amérique du Nord, les frais de notification sont la motivation principale. Leur coût est estimé en moyenne à 140 dollars par personne concernée, et les derniers cas de vol de données personnelles, largement médiatisés (Target, Sony), illustrent l'importance des enjeux financiers lorsqu'il faut faire des notifications individuelles.

En revanche, en Europe, les assurés recherchent davantage la garantie des pertes d'exploitation et de la reconstitution des données. Certaines institutions financières démontrent à travers l'existence d'un contrat de cyber-responsabilité qu'une partie de leurs risques opérationnels est transférée à un tiers solvable et obtiennent ainsi une réduction de leur niveau de capitaux propres réglementaires. Cela pourrait plaider en faveur de la multiplication des contrats de cette nature achetés par des banques ou des sociétés d'assurance, selon leur politique de gestion des risques opérationnels.

L'harmonisation des législations dans les pays économiquement développés devrait entraîner une certaine uniformisation des motivations d'achat, d'autant que les entreprises sont souvent confrontées à des obligations qui varient selon les pays où elles vendent leurs produits et en fonction de la protection dont bénéficient leurs clients.

Un processus de souscription long et complexe

Néanmoins, nous constatons que le processus de souscription de tels contrats reste long et complexe. Le premier contrat mis en place en France a nécessité dix-huit mois de négociation ; désormais il n'est pas rare de travailler pendant un an sur un tel projet. Cela est dû quelquefois à la difficulté de réunir l'ensemble des informations nécessaires auprès des directions des services informatiques (DSI) mais aussi à celle de trouver un budget additionnel pour le département assurance.

Cependant, l'intensification de la communication des autorités étatiques en charge soit de la sécurité du territoire, soit du développement économique, ajoutée à la médiatisation de certains cas de piratage informatique et de fraude, a commencé de sensibiliser les directions générales des entreprises à ce sujet et mis en exergue sa dimension stratégique. De ce fait, certains arbitrages budgétaires consacrent désormais une part plus significative à l'achat d'une garantie d'assurance parmi l'ensemble des moyens de prévention dont se dote l'entreprise.

La tendance de ces dix-huit derniers mois est donc une plus grande demande de cotation de la part d'entreprises de toute taille, alors que les premières demandes en France provenaient essentiellement de très grands groupes.

Cette tendance est également favorisée par la multiplication des offres des assureurs. Actuellement onze sociétés proposent des garanties de cyber-responsabilité en France, représentant un total théorique de capacité de 355 millions d'euros, alors qu'en 2010 seuls deux ou trois acteurs étaient présents sur ce marché. Il faut y ajouter les capacités du marché de Londres avec lesquelles nous pouvons mobiliser 100 millions d'euros supplémentaires. Cependant, en fonction de l'activité du souscripteur du contrat, cette capacité théorique n'est pas toujours facilement mobilisable.

Le marché de l'assurance cherche encore son équilibre entre la réponse aux besoins des entreprises et ses propres enjeux de création d'un portefeuille de risques nouveaux. Nous observons des politiques relativement différentes d'une société à l'autre, qui peuvent se résumer, d'une part, par l'apport d'une large capacité (25 M€ et au-delà) et la volonté de faire croître le portefeuille très rapidement afin d'être en mesure d'assumer les premiers sinistres d'intensité sans déséquilibrer l'ensemble des comptes d'un département de souscription ; d'autre part, par une politique plus prudente consistant à mesurer la capacité portée par risque (maximum 10 ou 15 M€) dans le même but que précédemment indiqué.

Cependant, la compétition nouvelle entre les assureurs dans ce type de garantie les oblige à adapter leur politique de souscription pour rester au plus près du marché. L'agilité et la capacité d'innovation des uns et des autres sont donc particulièrement sollicitées.

Un autre défi auquel sont soumis les assureurs est celui de la réactivité nécessaire en cas de survenance du sinistre. Une attaque informatique, que ce soit par déni de service ou par piratage de données, déclenche nécessairement un processus de gestion de crise au sein des entreprises. La demande de ces dernières porte donc aussi sur l'accompagnement de l'assureur dans ces moments. Ce sujet est extrêmement sensible pour les établissements de taille intermédiaire (ETI), souvent mal préparés à la gestion de crise et où il n'existe pas de plan de continuité d'activité intégrant pleinement la dimension de l'indisponibilité des systèmes d'information après une attaque logique. L'indisponibilité après un événement accidentel de type incendie ou inondation est bien mieux appréhendée par des moyens de secours et la redondance des systèmes. Néanmoins, les grands groupes sollicitent aussi le soutien de leur assureur dans une telle situation car ils souhaitent pouvoir profiter d'un retour d'expérience. Il faut donc avoir anticipé ces besoins pour pouvoir être efficace au moment de la survenance du sinistre.

L'adaptation des contrats existants

Il convient aussi d'adapter quelques fondamentaux des contrats d'assurance pour traiter les situations où l'assuré n'a pas immédiatement intérêt à faire cesser une attaque dans le but d'en trouver les auteurs et de parfaitement comprendre l'étendue des dommages, voire d'être capable de continuer à produire. Les autorités de police et de justice peuvent aussi, dans les mêmes buts, exiger que les causes d'un sinistre ne soient pas immédiatement stoppées. Le principe indemnitaire des contrats d'assurance doit alors être compris intelligemment par les parties. Seuls le dialogue et une collaboration efficace permettent dans ce cas-là de gérer la situation. Ces enjeux sont particulièrement sensibles pour les opérateurs d'importance vitale (OIV), soumis à une réglementation stricte et impérative pour eux-mêmes et leurs sous-traitants (voir encadré ci-dessous).

Les fondamentaux

• Donnée personnelle : tout ce qui permet d'identifier directement ou indirectement une personne. Cela comprend les éléments des dossiers médicaux tels radios, groupe sanguin mais aussi l'ADN. Définie à l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et libertés.

• Donnée confidentielle : toute donnée frappée d'un accord de confidentialité.

• PCI DSS : *Payment Card Industry Data Security Standard*. Il s'agit d'une norme de sécurité des données créée par le Conseil des normes de sécurité PCI.

Le Conseil des normes de sécurité PCI est un forum international ouvert, lancé en 2006, responsable du développement, de la gestion, de l'éducation et de la sensibilisation aux normes de sécurité PCI, dont :

– la norme de sécurité des données (DSS),

– la norme de sécurité des données d'application de paiement (PA-DSS),

– les besoins liés au service de saisie du PIN (PED).

L'organisation a été fondée par American Express, Discover Financial Services, JCB International, MasterCard et Visa Inc.

• OIV : opérateur d'importance vitale. Notion créée par la loi de programmation militaire du 18 décembre 2013.

Certains gestionnaires des risques estiment que le principe indemnitaire limite la portée des garanties de la cyber-assurance et militent pour une évolution des contrats vers une indemnisation forfaitaire

préagréée. Il s'agit presque d'une révolution du fonctionnement des contrats d'assurance, un pas que les assureurs n'ont pas encore franchi. La notion de valeur d'une donnée est d'ailleurs en mutation constante selon la date à laquelle celle-ci est collectée et l'évolution sociétale, voire sociologique, des notions de vie privée et de confidentialité. Il est fort probable que les générations ayant grandi avec les réseaux sociaux ne valorisent pas les données personnelles de la même façon que leurs aînés. La fluctuation d'une valeur intangible oblige les assureurs à revoir leurs bases actuarielles d'évaluation des risques.

Par ailleurs, l'interconnexion des systèmes informatiques entre plusieurs entreprises pour les besoins du travail, y compris par Internet, ou par le recours à la sous-traitance ou à l'hébergement des données dans les réseaux partagés, entraîne pour les assureurs des risques de cumul difficiles à appréhender. Un seul événement peut avoir des répercussions sur un nombre incalculable de clients, voire entraîner la mise en jeu de plusieurs garanties telles que les contrats de responsabilité civile exploitation, de dommages aux biens, de fraude, de kidnapping et rançon et de responsabilité civile des mandataires sociaux. La prise en compte de cette dimension influence bien évidemment les politiques de création de portefeuille évoquées ci-dessus. Cela prouve aussi que la frontière entre les différentes natures de risque n'est plus aussi bien délimitée qu'elle a pu l'être.

L'étude détaillée des risques

Enfin, le dernier écueil des assureurs est de ne pas couvrir, par inadvertance ou par manque d'analyse préalable, des risques qu'ils ne souhaitent pas assurer. La fraude à la carte bancaire en est la parfaite illustration. Peu d'assureurs acceptent de couvrir les banques et le groupement d'intérêt économique (GIE) des cartes bancaires pour ce risque, alors que la principale donnée dérobée lors d'un vol de fichier est le numéro de carte servant à faire des achats frauduleux.

Cela démontre que les assureurs doivent à la fois prendre en compte l'ensemble des conséquences d'une atteinte aux systèmes d'information et de la perte des données dans leur tarification, mais aussi étudier l'impact d'un dysfonctionnement des systèmes informatiques dans l'ensemble des autres garanties proposées dans les différents contrats.

La mise en place d'un contrat de cyber-assurance passe par une étude détaillée. L'entreprise devra ainsi remplir des questionnaires de plusieurs pages expliquant le nombre et la qualité des données détenues, les mesures de sécurité destinées à les protéger (cryptage, autorisation d'accès à des données en interne, surveillance des personnels), le détail des sinistres précédents ainsi que l'architecture informatique et les sécurités physiques et logiques mises en place. Ces éléments sont fréquemment complétés par une réunion de présentation des risques organisée conjointement avec la direction de la sécurité des systèmes informatiques et le responsable des assurances.

Le paradoxe vers lequel tend le marché de la cyberassurance est que les risques liés à une atteinte aux systèmes informatiques ne sont précisément étudiés que lorsqu'il s'agit de proposer un contrat, alors que les branches d'assurance plus classiques telles que les dommages ou la responsabilité civile seront sans doute rapidement contraintes d'inclure davantage ces notions dans leurs demandes d'information, ces contrats garantissant aussi, en partie, les conséquences d'une défaillance des systèmes d'information. Le pilotage automatisé des chaînes de production en est le meilleur exemple. Ainsi, l'évolution des méthodes de travail modifie les causes des événements garantis, et cela a nécessairement une conséquence directe sur le coût des sinistres indemnisés.

De plus, la position d'une chambre de la Cour de cassation qui accorde à une donnée la valeur d'un bien [1] pourrait entraîner l'ensemble d'une profession à revoir ses classiques à propos des notions de bien matériel et immatériel, et donc l'objet même de certaines garanties dont l'intention initiale était différente. Nous sommes cependant encore dans le cadre d'une prospective, car la décision mentionnée ci-dessus n'a pas été publiée au Bulletin de la Cour de

cassation. Il ne peut donc s'agir d'une position de principe définitive.

L'exposition aux risques des entreprises est en mutation, et les assureurs sont confrontés à un risque systémique et très contagieux d'une ampleur sans précédent qui les contraint à faire évoluer les contrats proposés, que ce soit par la création de garanties nouvelles ou par l'adaptation de celles que nous connaissons.

Note

1. Cour de cassation, chambre criminelle, 22 octobre 2014, pourvoi n° 13-82.630 : http://www.legifrance. gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000029631597

Cyberassurance : offres et solutions

Didier Parsoire

Responsable de souscription « cyber », SCOR Global P&C

Le monde est entré dans l'ère numérique. L'information devient vitale pour les entreprises. Internet démultiplie les échanges mais aussi les risques au sein du cyberespace. Les atteintes aux données et aux systèmes d'information (SI) se font plus sophistiquées et causent de plus grands dommages aux entreprises.

Face à ces risques, le marché de la cyberassurance, né il y a une quinzaine d'années, a véritablement pris son envol aux États-Unis vers la fin des années 2000 sous l'impulsion réglementaire. Le marché européen est, lui, encore naissant. L'offre de réassurance est balbutiante en raison du manque d'outils destinés à contrôler les accumulations de risques. Ce marché possède un fort potentiel de croissance dû aux enjeux qui occupent les entreprises et les gouvernements. Il lui faut néanmoins gagner en maturité sur toute la chaîne : de la gestion du risque par les entreprises à la mesure des expositions et des concentrations de risques par les assureurs et les réassureurs, en passant par la détermination du risque transférable au marché. Une véritable expertise doit se développer chez tous les acteurs pour en faire un marché pérenne.

Chaque année, la quantité des informations stockées sous forme numérique dépasse le volume du savoir humain qui nous est parvenu avant l'ère digitale. À la révolution industrielle succède la révolution numérique. L'information est la nouvelle matière première des agents économiques. Elle est collectée, transformée, stockée, échangée. Elle est le substrat d'une grande partie des produits et services que nous consommons. Dans cette nouvelle ère, l'ordinateur remplace la machine-outil ou en prend tout au moins le contrôle. Cette révolution des usages a été rendue possible par un développement exponentiel des technologies. La puissance de calcul et les capacités de stockage sont à la portée de tous, à moindre coût. Surtout, Internet et les infrastructures de communication ont permis, par la circulation planétaire de l'information, de décupler l'efficience des organisations et des processus.

La « cybernétique » a désigné, dès le milieu du XXe siècle, la science naissante de l'information et des automatismes. Aujourd'hui, nous en avons gardé l'abréviation « cyber », dérivée du mot grec *kubernan* signifiant « gouverner », que l'on décline à l'envi pour désigner les acteurs, les concepts et les objets de ce nouvel espace numérique.

Cyber-risques : un large éventail de menaces

Dès lors que l'information et son traitement innervent l'économie et les entreprises, le bon fonctionnement des systèmes informatiques est devenu capital. L'interconnexion offerte par les réseaux d'information a rendu de surcroît ces systèmes vulnérables aux attaques extérieures. Ainsi, le développement d'Internet a ajouté la menace intentionnelle au risque de nature accidentelle qui prévalait jusqu'aux années 1990.

Cette menace progresse et s'organise au fur et à mesure que l'information croît en volume et en valeur. Le « hacker » solitaire a fait place à la cybercriminalité, au cyberespionnage, au « hacktivisme » ou au cyberterrorisme, qu'ils soient le fait d'organisations ou d'États. Les motivations sont multiples : atteinte aux actifs tangibles ou intangibles de l'entreprise, intelligence économique ou géostratégique, gain financier… Les stratégies déployées (déni de service, défiguration de site Internet, logiciels malveillants, *phishing*, ou « hameçonnage », pour soutirer des informations, etc.) évoluent sans cesse et s'appuient sur des outils technologiques toujours plus sophistiqués et plus accessibles pour créer les vecteurs d'attaque. Surtout, les assauts les plus pernicieux révèlent un degré de préparation très élevé reposant sur une connaissance fine de l'objectif via l'ingénierie sociale, l'employé négligent ou indélicat.

D'une façon ou d'une autre, l'attaquant va exploiter certaines vulnérabilités identifiées de la cible. Là résident les cyber-risques. Et leur survenance peut mettre à mal l'entreprise non préparée : vol de millions de données de clients, divulgation de données sensibles de l'entreprise, demande de rançon (cyberextorsion), etc. Ces événements nécessitent une gestion de crise qui n'est pas sans rappeler celle engagée pour le rappel de produits défectueux ou en cas de demande de rançon à la suite du kidnapping d'employés ou de dirigeants.

C'est bien à ces nouveaux risques que tente de répondre le marché de la cyberassurance depuis l'avènement d'Internet, il y a plus d'une quinzaine d'années.

L'actualité récente, qu'il s'agisse des « mégafuites » de données survenues ces derniers mois ou des révélations de la mainmise des États sur nos données privées, oblige les différents acteurs de ce marché – assurés, courtiers, assureurs et réassureurs, mais aussi pouvoirs publics – à reconsidérer la nature du risque et les réponses qui peuvent être apportées.

Les différentes motivations d'achat de cyberassurance

La cyberassurance reste aujourd'hui un marché essentiellement nord-américain. Environ deux milliards de dollars de primes ont été collectés aux États-Unis en 2014, quand le marché européen en comptabilisait six fois moins. Encore faut-il s'entendre sur le décompte des primes : plus de la moitié de celles-ci proviennent de contrats combinant des garanties « cyber » et responsabilité civile (RC) professionnelle, en particulier pour les entreprises du secteur des TMT (technologies, médias, télécommunications). Ces deux marchés révèlent des dynamiques respectives très différentes.

Le catalyseur du développement de la demande aux États-Unis a été la mise en place par la plupart des États de réglementations visant à protéger les particuliers contre la violation de données à caractère personnel. Aujourd'hui, seuls trois États n'en sont pas encore dotés. Si les modalités diffèrent d'un État à l'autre, les entreprises sont dans l'obligation d'avertir les personnes concernées par les fuites de données, sous peine de sanctions. Par ailleurs, depuis 2011, la Securities and Exchange Commission (SEC) impose aux entreprises cotées de déclarer toute exposition significative aux cyber-risques et tout cyberincident majeur. Conjugué à l'importance des *class actions* (« actions de groupe »), cet environnement a conduit au développement de contrats « cyber » couvrant la

responsabilité des entreprises en cas de fuite de données (*data breach*) ainsi que les frais de notification aux tiers et de gestion de crise. Ce marché a vraiment pris son essor à la fin des années 2000.

En Europe, le cadre réglementaire actuel n'est pas le même. Il impose la notification de violations de données personnelles par les seuls opérateurs de communications électroniques (Internet, téléphonie) aux autorités nationales (la Cnil en France) et, dans certains cas, aux personnes concernées. Surtout, les sanctions financières sont bien moins lourdes qu'aux États-Unis. D'autre part, la possibilité (ou la culture) des actions de groupe est encore naissante. Dès lors, les entreprises se tournent en général plutôt vers la protection de leurs intérêts propres en mettant l'accent sur la couverture des incidents de sécurité de leur système d'information et de la perte d'exploitation qui en découle.

Des différences existent aussi entre l'Europe et les États-Unis relatives au niveau des limites d'assurance des contrats « cyber » spécifiques. Si elles peuvent atteindre 200 à 300 millions de dollars aux États-Unis, elles restent pour le moment inférieures à 150 millions d'euros en Europe. De même, le taux de pénétration des cyberproduits se distingue entre ces deux marchés. Il est assez difficile à établir précisément et dépend de la taille des entreprises, mais on estime qu'il se situe, selon les secteurs d'activité, entre 10 % et 50 % aux États-Unis, les institutions financières et le secteur de la santé en étant les principaux acheteurs. En Europe, le taux d'achat est bien moindre.

Les cyberassureurs : plusieurs générations d'acteurs

Le marché de la cyberassurance rassemble des acteurs de profils très différents : des assureurs généralistes, des assureurs spécialisés, des agences de souscription, des syndicats et consortiums du Lloyd's.

Quelques acteurs comme AIG, ACE ou Beazley ont été parmi les premiers du marché. Ils ont développé une offre internationale diversifiée combinant couverture d'assurance et assistance aux clients (évaluation des risques, gestion de crise). La plupart des autres acteurs ont émergé aux États-Unis et sur le marché de Londres lors des dix dernières années.

Plusieurs assureurs déclinent maintenant des produits pour l'Europe. Ces derniers mois, une nouvelle génération de « pools » et d'agences de souscription se positionne sur des produits ou des services nouveaux : protection des infrastructures industrielles, offre combinant assurance et service de détection d'incidents. Pour compléter le panorama, il faut aussi compter quelques réassureurs intervenant en facultative ou sur le marché direct. Au total, entre cinquante et soixante acteurs, présents aux États-Unis ou en Europe, interviennent sur le segment de l'assurance des grands comptes ou des PME.

Les capacités offertes varient de 5 millions de dollars à 100 millions de dollars et peuvent être supérieures pour certains pools. Le cœur de marché se situe probablement entre 10 millions de dollars et 15 millions de dollars, et, en pratique, peu d'acteurs ont réellement engagé à titre individuel plus de 25 millions de dollars à ce jour.

S'agissant plus spécifiquement du marché français, on recense actuellement onze acteurs d'assurance offrant une capacité théorique globale supérieure à 300 millions d'euros : ACE, AIG, Allianz, AXA Corporate Solutions, Beazley, CNA, Hiscox, Munich Re CIP, Swiss Re Corporate Solutions, XL, Zurich.

La cyber-réassurance en devenir

Jusqu'à récemment, les capacités engagées et la taille des portefeuilles « cyber » ne justifiaient pas l'appel à la réassurance. Cependant, la demande croît depuis quelques années. La cession des cyber-risques, quand elle a lieu, se

fait pour l'essentiel par extension des traités de RC professionnelle. On a vu aussi apparaître quelques traités de cyber-réassurance spécifiques principalement sur base proportionnelle pour accompagner le développement de cédantes sur ce segment. Le caractère mixte des contrats « cyber » (dommages et responsabilité) en rend la cession quelque peu difficile.

Aujourd'hui, la taille des portefeuilles et la gestion des cumuls de risques conduisent les assureurs à rechercher des protections de fréquence (*stop loss*) ou de type catastrophe. Les cybersinistres pouvant potentiellement impliquer des contrats traditionnels (dommages, RC professionnelle ou RC des mandataires sociaux, fraude, etc.) en sus des contrats spécifiques, on voit aussi apparaître des demandes de protection « clash » multilignes.

Il n'y a pas aujourd'hui de modélisation crédible ni de scénarios permettant la quantification des cumuls de cyber-risques. Par ailleurs, les critères spatiaux ou temporels habituels ne se révèlent pas pertinents pour définir un « cyberévénement », puisque Internet se joue des frontières et que les cyberattaques sont parfois découvertes plusieurs mois après avoir été perpétrées. Enfin, il est très rare de pouvoir remonter à la source de l'attaque. Un immense chantier s'ouvre donc sur l'évaluation et le contrôle des cumuls de risques. Le développement de l'offre de réassurance en dépend.

L'assurance des cyber-risques en quête de maturité

Un fort potentiel de demande...

Une conjonction de facteurs crée un fort potentiel de demande pour la cyberassurance.

Tout d'abord, les entreprises sont toujours plus dépendantes des technologies de l'information et, dans le même temps, éprouvent une difficulté grandissante à contrôler l'information. Externalisation des prestations informatiques, développement du *cloud*, traitement de plus en plus complexe de l'information, notamment via les approches « *big data* », nouveaux usages – réseaux sociaux, « *Bring your own device* » (Byod) – et relation au monde physique via les objets connectés, toutes ces tendances dispersent l'information, en démultiplient les canaux d'accès, amplifient les risques existants et en créent de nouveaux (dommages matériels ou corporels).

Parallèlement, les gouvernements expriment un intérêt croissant pour le cyberespace, devenu enjeu de guerre économique et politique. Les menaces terroristes sont le moteur (et parfois le prétexte) d'un contrôle croissant des échanges sur Internet. La protection des données personnelles se développe. Un règlement européen est en cours de discussion et pourrait s'avérer contraignant pour les entreprises en ce qui concerne la notification aux autorités en cas de violation de données personnelles. Les États-Unis réfléchissent à une harmonisation fédérale des multiples réglementations existantes en la matière.

La gouvernance des entreprises est aussi à l'ordre du jour tant les attaques récentes ont montré les risques qu'elles font porter sur leur existence même.

La préservation des infrastructures critiques (eau, énergie, services financiers, transports, etc.) fait l'objet d'une attention croissante de tous les États. En France, la loi de programmation militaire comporte des dispositions spécifiques en matière de cybersécurité s'appliquant aux opérateurs d'importance vitale (OIV).

Enfin, la série sans précédent des cyberattaques majeures survenues ces derniers mois révèle l'ampleur de la menace et suscite une sensibilisation accrue au risque : Target, JPMorgan Chase, Home Depot, Sony, Anthem, etc., soit des centaines de millions de données dérobées, des attaques sophistiquées et des motivations diverses (gain financier, atteinte à l'entreprise). L'actualité récente a montré l'asymétrie de moyens entre attaquants et défenseurs, et les difficultés, voire le manque de préparation, des

entreprises pour faire face à ces attaques. Les pertes potentielles sont considérables et peuvent facilement dépasser les limites actuelles de l'assurance, sans même parler des risques inassurables (perte d'image, par exemple).

... mais des défis à surmonter

Ce contexte offre des opportunités réelles au marché de l'assurance et de la réassurance. Pour autant, un grand nombre de défis doivent encore être surmontés.

En effet, les entreprises éprouvent encore des difficultés à gérer leurs risques et à évaluer leurs besoins d'assurance. La gestion du cyber-risque est encore trop fragmentée entre de multiples directions (informatique, risk management, juridique, etc.) et manque bien souvent d'une vision globale des actifs et processus à risque. L'apport des contrats « cyber » spécifiques par rapport aux contrats traditionnels n'est pas toujours clairement identifié par les acheteurs d'assurance, et des doublons de garantie peuvent exister.

De leur côté, les assureurs peinent à évaluer et à tarifer les risques. Il existe un manque de données historiques sur les sinistres et incidents, renforcé par la réticence des entreprises à partager l'information. D'autre part, l'évolution rapide des technologies et des profils de menace rend difficile l'extrapolation à partir de l'expérience passée. Une autre difficulté à laquelle se heurte l'évaluation de l'assureur est l'absence de référentiel ou de standard partagé par les entreprises en matière de gestion du risque.

Par ailleurs, l'identification des cumuls d'engagement et des scénarios catastrophes reste difficile. Des exemples récents l'illustrent : une cyberattaque peut potentiellement affecter plusieurs contrats d'assurance traditionnels (RC professionnelle, RC des mandataires sociaux, dommages, RC générale, etc.) en sus ou en l'absence de couvertures « cyber » spécifiques. De plus, les risques de sinistres sériels à grande échelle sont bien réels : interconnexion des systèmes et standardisation des produits informatiques créent un risque de propagation virale, et l'externalisation par le *cloud* génère des concentrations de risques chez les fournisseurs. Nous l'avons déjà évoqué, le marché manque aujourd'hui de données, de modèles et de scénarios pour évaluer ces cumuls.

En dernier lieu, on observe un manque d'expertise chez l'ensemble des acteurs concernés. La pénurie d'experts en cybersécurité est patente dans le tissu industriel en général. Elle est encore plus évidente chez les acheteurs d'assurance, les porteurs de risque et les intermédiaires. La science des cyber-risques n'a pas encore vraiment pénétré le marché de l'assurance.

Conclusion

On le voit, même si ce marché a maintenant une quinzaine d'années d'existence, la cyberassurance et plus généralement la gestion du cyber-risque doivent se réinventer à la lueur des changements intervenus dans le paysage des risques sous-jacents.

L'assurance et la réassurance ne peuvent assumer le risque d'entreprise ou se substituer à une gestion optimisée des risques, mais elles joueront pleinement leur rôle dans la chaîne de gestion et de portage du risque dans la mesure où l'information sera organisée et partagée entre les différents acteurs afin de permettre une meilleure évaluation des risques et un contrôle des cumuls d'engagement. Le marché sera alors à même de structurer les capacités nécessaires, de développer des solutions spécifiques et d'adapter ses offres en fonction des différents segments d'exposition. Les États devront aussi s'impliquer dans la couverture des événements majeurs de type cyberterrorisme ou cyberguerre, qui dépassent par leur ampleur les capacités du marché.

La prise de conscience généralisée qui s'observe actuellement doit servir de catalyseur pour que non seulement les acteurs de marché mais aussi les pouvoirs publics définissent le cadre et les moyens du développement d'un marché pérenne de la cyberassurance.

3.

Survivre à des taux d'intérêt historiquement bas

INTRODUCTION

Philippe Trainar

Partout dans le monde, les taux d'intérêt n'ont jamais été aussi bas sur une aussi longue période de temps et jamais les marchés n'ont anticipé un retour à la moyenne aussi lent qu'aujourd'hui. Ceci est particulièrement vrai en Europe : si l'on prend comme référence les séries longues dont nous disposons sur les taux des obligations d'État à dix ans, ou les « *consols* » pour l'Angleterre, ceux-ci n'ont jamais été aussi bas qu'aujourd'hui en Europe et, aux États-Unis, ils sont à peine supérieurs à leur niveau le plus bas (qui s'est situé à 1,5 - 1,6 % après la guerre et au plus fort du *quantitative easing*). En outre, les taux des obligations d'État les moins risqués en Europe continentale sont désormais négatifs sur l'essentiel de la courbe des taux : jusqu'à sept ans en Allemagne. Enfin, les marchés n'anticipent pas de remontée rapide des taux, ni en Europe ni aux États-Unis : les taux à terme font ressortir des taux à trois ans encore négatifs dans deux ans en Allemagne et des taux à dix ans qui n'augmenteraient pas de plus de 20 points de base à cet horizon. Nous sommes entrés dans une ère de taux durablement bas et proches de zéro, voire négatifs, en Europe. À tout le moins, ceci est une hypothèse tout à fait raisonnable aujourd'hui alors qu'elle aurait paru tout simplement folle il y deux ou trois ans.

Cette situation change totalement la donne de la gestion de l'assurance et de la réassurance. Des situations financières qui n'étaient, il y a encore peu, pas envisageables même dans les scénarios les plus extrêmes sont devenues la normalité du jour : les banquiers centraux, qui excluaient les taux nominaux négatifs, en sont devenus les promoteurs et les marchés qui anticipent désormais une persistance de cette situation dans les années à venir, dans le cadre d'un retour à la moyenne très étalé dans le temps, leur ont emboîté le pas. Sur quelle normalité doivent compter les assureurs ? Quelles situations extrêmes doivent-ils envisager ? S'ils se réfèrent aux données empiriques du passé, ils ne peuvent qu'en conclure à l'anormalité de la situation actuelle, qui correspond à une probabilité inférieure ou égale à 0,5 %, et à un retour vers la moyenne d'autant plus rapide et brutal que l'on s'en est violemment écarté. Or, les marchés pensent justement le contraire. Et, peut-on expliquer à un conseil d'administration que, sur la base des données empiriques disponibles, l'on devrait a priori exclure, dans les circonstances actuelles, toute poursuite de la baisse des taux d'intérêt dans la zone des taux négatifs ? Tels sont les dilemmes de la gestion de l'assurance aujourd'hui. Ces dilemmes sont particulièrement délicats à traiter dans la mesure où le risque en assurance et en réassurance ne s'apprécie pas par rapport à l'écart type mais par rapport aux situations correspondant à un taux de retour de 1 sur 200 ans, des situations extrêmement rares, qui testent donc les limites de nos expériences et de nos connaissances, tout particulièrement quand la situation de départ se situe d'ores et déjà aux limites de ce que nous connaissons.

Dans ces situations, les risques prennent eux-mêmes une tournure particulière. La politique monétaire agressive menée actuellement réduit peut-être le risque de crédit, puisqu'elle rend plus aisé le refinancement des agents, mais elle accroît en contrepartie le risque macroéconomique, que l'on peut mesurer d'une part par l'écart du taux sans risque, entendu sans risque de crédit, par rapport au taux d'équilibre, d'autre part par le risque de retour brutal de ce taux vers sa valeur d'équilibre. De ce point de vue, les

valeurs dites de « *safe haven* », qui bénéficient actuellement d'une prime négative, ne sont pas des valeurs aussi sûres qu'on pourrait le penser car elles sont probablement les plus exposées à ce risque de correction brutale du niveau des taux. La dette allemande est donc particulièrement risquée de ce point de vue. De même, la hausse des actions et de l'immobilier en Europe est largement spéculative dans la mesure où elle est exclusivement imputable à la baisse des taux et non aux perspectives de croissance : on peut estimer ainsi qu'un point de baisse des taux d'intérêt à dix ans induit une hausse des actions de 7 % en moyenne (3 à 11 %). Étant exposée à un risque de correction sévère en cas de retour à la normale des taux d'intérêt, si celle-ci n'est pas accompagnée d'un redressement équivalent du taux de croissance de l'économie, ce qui est peu probable, la valorisation actuelle des actions est donc extrêmement fragile. Et pourtant, les garanties minimales, notamment les garanties en capital, accordées dans le cadre des contrats d'assurance vie imposent aujourd'hui aux assureurs de rechercher plus de risques à l'actif pour couvrir ces garanties, sachant que les titres à revenu fixe n'offrent plus de rémunération suffisante.

Il est clair que les banquiers centraux ont fait le choix des gouvernements et des banques contre les assureurs, qu'ils l'ont fait dans des proportions totalement inimaginables précédemment et que ce choix a des conséquences importantes pour la gestion des actifs et des passifs en assurance.

Sylvain de Forges souligne la radicale nouveauté de l'environnement financier actuel et recommande, au nom du principe de réalité, de ne pas chercher à échapper aux conséquences que ce nouveau monde implique pour l'assurance. Ceci induit d'accepter de revoir notre relation au risque, tant du côté des épargnants que du côté des intermédiaires financiers eux-mêmes.

Benjamin Serra estime que les taux durablement bas entament progressivement la solidité financière des assureurs. Il souligne toutefois que les situations nationales sont très diverses, pointant un risque particulièrement élevé dans le cas de l'assurance vie allemande par opposition à l'assurance vie française. Les assureurs s'adaptent en baissant les taux garantis, en privilégiant les unités de compte ou de nouveaux produits, en se diversifiant et en prenant plus de risques à l'actif.

Stéphane Dedeyan souligne l'intérêt de l'euro-croissance dans le cadre de la conjoncture actuelle. Il estime qu'il donne un nouveau cadre à l'assurance vie française qui devrait lui permettre d'affronter dans la durée un environnement de taux bas, d'améliorer les perspectives de rendement des épargnants vie et de renforcer la capacité de l'assurance vie à financer l'économie.

Emmanuelle Laferrère et ***Pierre de Villeneuve*** constatent que les fonds en euros ne constituent plus la bonne réponse aux besoins des assurés et que l'euro-croissance doit prendre le relais pour les placements à long terme. La question cruciale devient donc celle du passage des fonds en euros aux fonds euro-croissance : il est important que les transferts de richesse des uns vers les autres se fassent dans des conditions favorables et incitatives.

Eric Bertrand et ***Arnaud Faller*** explorent les moyens qui, dans la *terra incognita* des taux d'intérêt bas où nous nous trouvons, permettraient de gérer la matière obligataire pertinemment. Ils proposent notamment d'améliorer la diversification, d'accroître la flexibilité, de développer les investissements en devises étrangères et de retrouver du thêta positif (par des stratégies exploitant les « *strangles* »).

Fabrice Rossary part des trois grandes familles de stratégies de gestion d'actifs (les stratégies de portage, les stratégies directionnelles et les stratégies d'arbitrage), pour conclure que la seule action possible pour accroître le rendement consiste à combiner l'allongement de la duration de l'actif, la prise de risques de crédit et de liquidité, l'arbitrage des bases, l'exposition au risque alternatif et l'introduction de classes d'actifs au remboursement non-prédéfini.

Taux bas : un monde nouveau

Sylvain de Forges

Directeur général délégué, AG2R La Mondiale

Les lignes qui suivent sont la reprise, mi-février 2015, d'une intervention faite le 28 août 2014 à l'université de l'Asset Management à Paris-Dauphine. Les évolutions, notamment de marché, connues depuis lors n'ont pas conduit à en modifier fondamentalement la structure ni l'argument – juste le début de la conclusion. Figurent parfois, entre crochets, des actualisations des données chiffrées.

Lorsque j'ai accepté, en mai 2014, d'intervenir sur ce thème, je n'imaginais pas – et nul dans cette salle ou hors de la salle ne l'avait à ma connaissance prédit – qu'aujourd'hui le taux à dix ans du Bund serait à 0,88 %, celui de l'OAT à 1,23, celui de l'Espagne à 2,19... [13/02/2015 : respectivement 0,33 ; 0,64 et 1,54 %...].

Le paysage que nous avons trouvé au retour de nos congés d'été est significativement différent de celui que nous avions laissé.

Je constate aujourd'hui un terrible consensus : ces niveaux de taux, sans précédents historiques connus, sont là pour durer. Du moins en Europe de la zone euro. La « pire » production que j'aie lue ces jours derniers, faite par une équipe pour laquelle j'ai de l'estime, n'exclut pas que cela puisse durer quinze ans. Il est passé ce temps, pas si lointain, où nombre d'experts, devant des niveaux de taux déjà considérés comme exceptionnellement bas, s'inquiétaient d'un « krach obligataire » guettant au coin de la rue. Et il est patent que, lorsque la BCE installe puis diffuse son analyse selon laquelle il n'y a pas aujourd'hui de « bulle » manifeste, je n'entends aucune voix qui le conteste.

Comment se fait-il... ?

Comment se fait-il que même les « Cassandre », dont je fus – ces caractères qui prédisent ce qu'ils redoutent –, n'aient pu prévoir la profondeur de ce mouvement ?

Des analyses de court terme existent : par exemple (publicité gratuite), dans un papier publié ce matin par l'équipe de Natixis, celle de Patrick Artus que tous nous connaissons. Il est rappelé que, il y a un an, le « consensus » anticipait pour aujourd'hui (fin

août 2014 donc) un taux à dix ans de 2,70 % aux États-Unis et de 1,9 % en Allemagne. Ce papier liste quatre raisons pour expliquer cet écart majeur entre prévision et situation : sous-estimation des effets de la forte croissance de la liquidité mondiale, modération du report des investisseurs vers les actifs risqués, surestimation de l'inflation et de la croissance, excès d'épargne de la zone euro… – toutes analyses de court terme. Nous savons que le problème est plus profond.

Oui, les taux sont excessivement bas. Oui, c'est l'image réfléchie d'un drame collectif. Et oui, ça peut durer longtemps. J'ai donc répondu à la question posée, au premier degré. Au second degré, je suis malheureux de dire et penser cela. Je me trouve dans une situation que je déteste : décrire une situation dépressive, dépression des personnes physiques, dépression des personnes morales que sont nos économies, l'économie française en particulier. Or la dépression, ça se soigne – pour les personnes morales comme pour les personnes physiques. Comment soigner celle-ci ?

Il nous faut accepter le principe de réalité

Si nul d'entre les experts n'a su prédire la situation actuelle, c'est donc que leurs outils sont inefficaces. Qu'on ne parle pas de nouveau paradigme : ce mot, qui fut très à la mode et l'est encore, est inacceptable ici. Paradigme est un terme technique de grammaire : « mot type donné comme modèle pour une déclinaison, une conjugaison » (ex. : *rosa* en déclinaison latine, aimer en conjugaison française). Nous n'avons pas de modèle type qui fonctionne – il n'y a pas de paradigme, il y a juste un nouveau monde, un inconnu dont la carte n'est pas dressée.

Le 26 août, avant-hier, paraissait dans *Les Échos* une interview de Michel-David Weill. Je cite : « les taux d'intérêts sont beaucoup trop bas. La norme des taux d'intérêts, c'est 3,5 % + inflation. Ça a toujours été comme ça depuis Florence ». Ça, ce peut être un paradigme. Il n'a plus cours, aujourd'hui.

Nous sommes dans un nouveau monde

Nous y entrons en situation dépressive, pour notre part – ce qui n'est pas le cas de tous nos partenaires ou concurrents. Nous n'en avons pas la carte. Il nous faut donc, après le principe de réalité, retenir le principe de modestie : admettre que nous ne savons pas nous affranchir des idées anciennes prouvées inefficaces, explorer le monde nouveau en donnant la priorité au pragmatisme sans tabou et au bon sens ; à des vertus de proximité. Et ceci pose trois questions :

- Que savons-nous de ce nouveau monde ?
- Que savons-nous de nous-mêmes ?
- Que pouvons-nous faire ?

Que savons-nous de ce nouveau monde

Nous en savons une ou deux choses. Dans ce nouveau monde, nous sommes en compétition avec des systèmes, ou plutôt des cultures, dont le référentiel est très éloigné du nôtre à de nombreux égards. Cela s'appelle la mondialisation, ou la globalisation pour prendre l'anglicisme. Ces systèmes sont différents des nôtres à deux égards très importants, notamment :

- leur relation au risque. Elle est très différente de la nôtre, en commençant par l'importance accordée à la vie humaine. Ce qui est chez nous ressenti comme un drame collectif ne l'est pas pour 80 % de nos compétiteurs. Sur tant d'autres plans aussi, qui se déclinent : l'appétence au jeu, une relative indifférence aux questions environnementales, l'acceptation de l'échec, mais aussi de la réussite. Je ne sais comment traduire, en chinois, ce « principe de précaution » qui est en France de nature constitutionnelle. Je comprends et respecte ce principe – dans son esprit du moins – mais je sais que c'est une exception culturelle, dans le monde réel globalisé ;

- leur relation au temps et à l'histoire. À leur histoire, si différente de la nôtre. Internet aidant, notre niveau objectif de prospérité a fait prendre conscience à une

partie, infime d'abord mais résolument croissante, de l'humanité qu'il existe, pour elle, une perspective. Une perspective dont nous doutons tellement pour nous-mêmes que nous avons le mauvais goût de dire, ou de laisser dire, ce doute à nos enfants. Cette perspective, c'est l'espoir ou l'espérance, la confiance dans les capacités humaines : l'avenir peut être, et donc sera plus faste que le présent. Il ne s'agit pas tant pour ces sociétés d'une « revanche » à prendre que, ce qui est infiniment plus efficace et au demeurant estimable, d'une espérance et d'une conviction. Après l'Asie du Sud-Est et la Corée, elles ont saisi la Chine. Elles saisissent le sous-continent indien, l'Amérique du Sud. Demain, ce sera l'Afrique. Je souhaite évidemment à ces sociétés l'avenir qu'elles désirent et pour lequel, progressivement, elles vont combattre avec une efficacité croissante.

Cette compétition nous effraie, car nous ne savons pas nous défaire de l'hypothèse d'un jeu à somme nulle : qu'elles progressent et nous perdrions ? Cette vue malthusienne n'est pas acceptable, le jeu est à somme très largement positive.

◆ Que savons-nous de nous-mêmes ?

Nous savons que nous avons développé une très forte aversion au risque. Et pour, malheureusement, de bonnes raisons dont je vais faire rapidement le tour.

• Ce monde est dangereux. Des risques anciens ou nouveaux émergent à tout instant, dans tous les ordres. Ressentis comme immédiats ou à effet long. Et ils s'additionnent :

– le risque démographique dans nos sociétés occidentales, qui induit chez chacun de nous une fuite vers la sécurité ;

– le risque de la compétition – j'en ai déjà parlé ;

– le risque environnemental – mes années passées chez Véolia m'autorisent à dire que le réchauffement est une réalité, que se disputer sur la question de l'origine des causes est une absurdité logique, car une absolue perte de temps et d'énergie, un refuge pour éviter d'affronter la seule question qui vaille, qui est « que pouvons-nous y faire ? », pour le futur qui commence aujourd'hui ;

– les risques sanitaires : Ebola après Sras et Creutzfeldt-Jakob, maladies neurodégénératives de plus en plus perçues et redoutées ;

– les risques dits « stratégiques » de disruption profonde : États islamiques en Syrie ou au Nigeria, doctrine Poutine, mer de Chine et quelques autres lieux… nous n'avons que l'embarras du choix ;

– et aussi, les risques de sécurité des systèmes complexes que nous avons développés, dont les flashs crashs ne sont qu'une des manifestations, les moins sévères.

• Nous savons aussi que l'un des principaux « *softeners* [1] » des situations précédentes, l'inflation, a aujourd'hui disparu. Ne le regrettons pas : puis-je rappeler que, il y a exactement un tiers de siècle, à l'automne 1981, la République émettait difficilement, à sept ans, au taux de 16,75 % ? Ce serait aujourd'hui… 0,7 % ? [0,2% en février 2015 ?] À moyen terme, il est peu probable que l'inflation redresse ne serait-ce que modestement la tête, disons jusqu'à ce niveau de 2 % si cher à nos autorités monétaires. Car, selon moi, ses deux composantes principales – prix des matières premières, inflation salariale – sont durablement plafonnées :

– la première parce que nous allons progressivement entrer dans des modèles économiques et techniques de plus en plus économes en ressources nouvelles, y compris dans le domaine énergétique. Nous en voyons déjà les premières manifestations – bâtiments, transports, gestion des déchets, aménagements urbains ;

– et la seconde pour la raison, exposée plus haut, de la mondialisation et de l'accès croissant de populations qui en sont aujourd'hui exclues à la prospérité et d'abord à l'entreprise et au marché mondial.

◆ Que pouvons-nous faire ?

Que nous faut-il faire ? Je ne vais pas entrer dans les débats si bien connus, si ardents et si difficiles, entre politique de l'offre et de la demande – nous savons bien que la réponse n'est pas binaire –, mais dans la recherche d'un équilibre dynamique entre les positions non pas antagonistes, mais complémentaires. Il est également inutile de revenir sur la nécessité d'adopter des réformes structurelles qui permettront, tout à la fois :

– de booster la compétitivité et la rentabilité des entreprises et d'inverser l'évolution du chômage, en particulier des populations jeunes, par un effort spécifique et entêté de formation ;

– et d'améliorer la performance de la dépense publique – ce qui n'est d'ailleurs qu'une variété du point précédent, tant il est vrai que le secteur public est, essentiellement, un prestataire de services au public ou de services publics, dont il va de soi qu'il faut renforcer la compétitivité et l'efficacité.

J'aimerais ici insister sur trois points.

• Il nous faut savoir nous affranchir des convictions, des mantras en vigueur dans le monde précédent. La bonne nouvelle est que, dans ce domaine, et avec toutes les hésitations naturelles qui nous assaillent, nous avons largement commencé. Je prends quelques exemples dans notre sphère des marchés : les grandes banques centrales ont su mettre en place des outils dont elles s'étaient interdit l'usage :

– de façon parfois symétrique au demeurant : la Fed intervient sur effets privés, la BCE intervient sur les titres publics, ce qui leur était symétriquement interdit jusqu'en 2007. Une autocensure est heureusement morte – non sans débats, bien sûr ;

– de même, devant la constatation que les modes traditionnels de transmission de la politique monétaire ne fonctionnent plus, l'institut d'émission européen innove : c'est aujourd'hui que les banques doivent lui faire parvenir une estimation de leur demande de TLTRO [2], T comme *targeted*, qui sera lancé le mois prochain, pour un encours qui pourrait dépasser 100 milliards d'euros. C'est une situation originale : la distribution de crédits bancaires sera directement subventionnée par des fonds publics. [Et, en février 2015, le QE [3] est bien le « successeur naturel » du TLTRO – capacité d'adaptation, là encore].

Nous revisitons aussi, d'une façon qui s'accélère depuis quelques semaines, les sagesses reçues en matière de finances publiques : l'analyse sur l'efficacité de la dépense, distinguant mieux par exemple entre budgets classiques et transferts.

Progressivement, notre intelligence de ce monde nouveau prend forme. Et un sourire : il y a peu d'années, l'ensemble de la doctrine considérait qu'il ne pouvait y avoir de taux nominaux négatifs, même à court terme – ou que ce serait l'Armageddon de la déflation chronique, pire encore que ce que fut 1929. Il n'est pas heureux que les taux courts [et maintenant longs, en février 2015] soient négatifs, il est heureux que nous n'en fassions pas le drame redouté il y a quelques mois.

• Il nous faut, non pas retrouver, mais bien trouver une relation efficace et non émotive avec la prise de risque. Trouver, dis-je, car ce serait nouveau en France, depuis deux siècles. Je prends ici un exemple dans mon environnement professionnel immédiat : l'épargne des agents économiques atteint des niveaux remarquables, mais cette épargne est placée dans des instruments les moins risqués possibles. Ceci est vrai des personnes physiques, les ménages et les patrimoines. Vrai aussi de personnes morales, parfois avec un encouragement implicite des régulations nouvelles qu'ont amenées les troubles de ce qu'on a appelé la crise de la finance. Bien évidemment, et heureusement, y-a-t-il de grandes exceptions à ce comportement moyen. Mais telle est bien la situation moyenne.

• Et il nous faut, avec pragmatisme puisqu'il n'y a pas de paradigme à disposition et utilisable, repartir de la

base, des entreprises. Faire tout ce qui est possible pour qu'elles puissent naître, se développer, et aussi résister aux difficultés qu'elles rencontrent. Un point particulier ici nous concerne dans nos métiers respectifs, et ce sera la fin de mon intervention que m'autorise mon activité au Medef : il nous faut nous assurer que, le cas échéant, et dans une analyse rationnelle, l'intermédiation financière au sens large mette à la disposition des entreprises des moyens nouveaux et pluriels de financement adaptés à la reprise que tous nous espérons.

Un renouveau indispensable pour un enjeu essentiel

Tout l'enjeu des prochains trimestres est qu'il n'y ait pas étouffement d'une reprise fragile par défaut de financements adaptés. C'est vrai en France – ce n'est pas vrai qu'en France, comme nous le savons tous. Chacun doit donc concourir au succès :

– les entreprises elles-mêmes, en se gérant au mieux, individuellement et collectivement (crédit inter-entreprises...) et en simplifiant leur structure financière ;

– les épargnants, en acceptant un allongement de la durée de leur épargne et l'accroissement de leur prise de risque (contrats eurocroissance, PEA-PME...) ;

– les intermédiaires, en proposant des produits simples et économes en frais de gestion : produits types, taille de programmes importante évitant une offre trop morcelée et permettant d'amortir les coûts fixes (charte euro-PP [4]…) ; mais aussi utilisation rationnelle des vastes possibilités offertes par les plateformes électroniques qui peuvent diminuer significativement les coûts d'accès et de traitement en B2C [5] ;

– les investisseurs, en trouvant une appétence nouvelle pour le risque justifiée par l'accès à une compétence renforcée sur l'analyse du couple risque/rendement dans un environnement où le taux sans risque est pratiquement nul, et en confirmant leur attrait pour des investissements dans l'économie dite « réelle » ;

– et, peut-être, aussi, les garants de la « sagesse prudentielle » : le système actuellement mis en place n'est-il pas, par endroits mais très visiblement, si vocalement hostile au risque qu'il a pour effet de convaincre les autres agents (épargnants d'un côté, mais aussi entreprises en commençant par les moyennes et petites), que toute prise de risque est une « folie pure » ?

Et cela alors qu'investir et entreprendre sont les deux faces d'un même pari, raisonné, sur un avenir à construire.

Conclusion

En ces premières semaines de 2015, nous croyons percevoir, à défaut d'une reprise franche, de premiers frémissements. Il nous faut éviter une situation de catch 22, où globalement une demande fragile, pour les entreprises moyennes et petites du moins, rencontrerait une offre elle-même sous contrainte non seulement pour les fonds propres mais aussi pour les financements courants, et a fortiori pour les éventuels investissements de développement. L'équilibre actuel est massivement sous-optimal, dirait M. Pareto.

Si nous savons évoluer le long des pistes que j'ai mentionnées et de nombreuses autres, si nous savons le faire avec persévérance sinon entêtement, alors, et même dans un univers notamment financier fort éloigné de la Florence du XIIIe siècle, alors en effet, pourrons-nous retrouver la situation décrite par Michel David-Weill : des taux d'intérêt à 3,5 % + inflation.

J'espère profondément – que Cassandre ait tort et se taise ! – voir cela avant ma propre retraite.

Mais celle-ci n'est pas pour tout de suite...

Notes

1. Adoucissant.

2. TLTRO : Targeted Longer Term Refinancing Operations *ou opérations de refinancement ciblées à long-terme, un système de prêt à long terme (4 ans) offert aux banques par la BCE.*

3. QE : quantitative easing *ou assouplissement quantitatif.*

4. Euro PP : Euro Private Placement, *opération de financement à moyen ou long terme entre une entreprise, cotée ou non, et un nombre restreint d'investisseurs institutionnels.*

5. B2C : Business to Customer. *Activités tournées vers le consommateur (à opposer à B2B :* Business to Business*).*

Les taux bas menacent-ils les assureurs européens ?

Benjamin Serra

Vice-President Senior Credit Officer, Moody's Investors Service

Les taux d'intérêt européens ont atteint des niveaux historiquement bas et resteront bas vraisemblablement de manière durable. Dans cet environnement, la solidité financière des assureurs, notamment celle des assureurs vie, s'affaiblira progressivement. Les assureurs français sont moins exposés que leurs homologues allemands, néerlandais ou scandinaves, mais ils sont aussi impactés par cette situation. Partout en Europe les assureurs prennent des mesures pour contrer la baisse des taux d'intérêt, mais ces mesures auront des conséquences multiples sur leur activité et leur rentabilité.

Quand le stress devient réalité

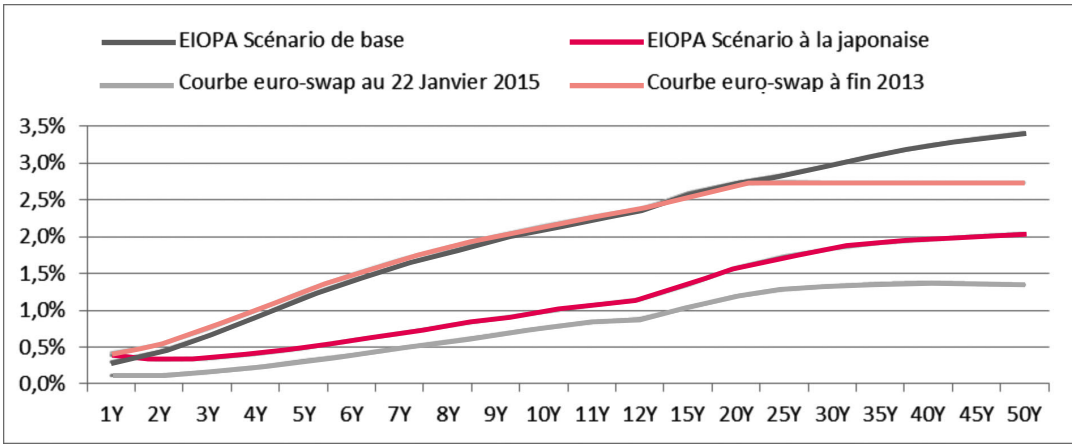
Le 22 janvier 2015, la Banque centrale européenne (BCE) a lancé un programme de rachat massif d'actifs. Cette politique monétaire non conventionnelle a fait plonger les taux d'intérêt de la zone euro à des niveaux historiquement faibles, et aucune remontée des taux n'est attendue à court ou moyen terme. Par ailleurs, les mesures prises par les banques nationales suisse et danoise en anticipation de la décision de la BCE (1) ont étendu cet environnement de taux extrêmement bas à pratiquement l'ensemble de l'Europe (2). D'aucuns diront que la BCE a mené l'Europe en bas taux.

Comme expliqué ci-dessous, ce scénario est très défavorable pour les assureurs. Un scénario de taux durablement bas, communément appelé « scénario à la japonaise », était par ailleurs l'un des scénarios de stress retenus par l'Autorité européenne des assurances et des pensions professionnelles (en anglais European Insurance and Occupational Pensions Authority ou EIOPA) lors de son exercice de stress tests réalisé en 2014 sur la base des données financières à fin 2013. Toutefois, comme on peut le voir sur le graphe 1 (p. 78), les taux ont aujourd'hui atteint des niveaux plus bas que ceux envisagés par l'EIOPA dans ses stress tests. Autrement dit, ce qui était considéré il y a peu de temps comme un stress est maintenant devenu une réalité.

Des taux bas affaiblissent la qualité de crédit des assureurs

Les assureurs investissent en grande majorité sur des titres obligataires (environ 80 % de leurs actifs). Le rendement de leurs actifs est donc fortement corrélé aux taux d'intérêt. Certes, les assureurs investissent en général à long terme, ce qui signifie que leurs portefeuilles incluent

Graphe 1 : Les taux ont atteint un niveau plus bas que dans le scénario de stress envisagé par l'EIOPA



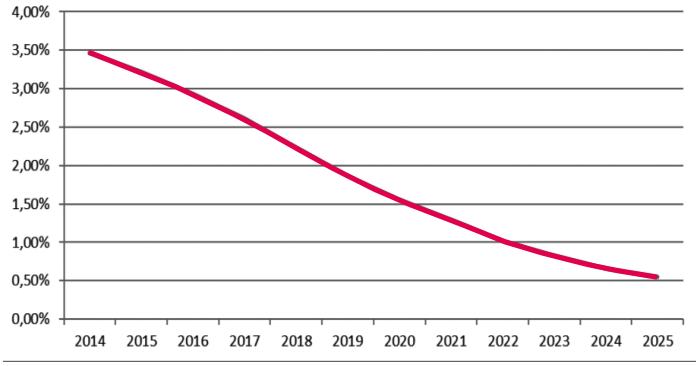
Sources : Bloomberg, EIOPA, Moody's Investors Service.

des titres anciens bénéficiant d'un rendement élevé, et la baisse des taux ne se répercute donc pas immédiatement en intégralité sur le rendement de leurs actifs. Mais une partie des actifs doit être réinvestie chaque année. Compte tenu de la baisse des taux continue depuis plusieurs années, le taux de réinvestissement est plus faible que le taux de rendement des actifs venant à échéance, ce qui diminue progressivement le rendement global des actifs de l'assureur.

À titre d'illustration, le graphe 2 présente l'évolution future du taux de rendement des actifs d'un assureur ayant une activité constante et investissant uniquement sur des OAT (3) de maturité dix ans (cet assureur réinvestit donc chaque année 10 % de son portefeuille et la duration de son actif est de 5,5 ans), en supposant que les taux d'intérêt restent stables entre 2015 et 2025.

La baisse du taux de rendement des actifs devrait être plus rapide pour les assureurs dommages, qui ont en général un actif de duration plus faible que celui des assureurs vie (de l'ordre de cinq ans ou moins pour les assureurs dommages contre de l'ordre de dix ans pour les assureurs vie), et qui réinvestissent donc chaque année une plus grosse part de leurs actifs. Toutefois, l'impact de la baisse des rendements sur la solidité financière des assureurs est, en général, plus fort pour les assureurs vie.

Graphe 2 : Évolution du rendement d'un portefeuille composé d'OAT dix ans en cas de stagnation des taux*



* Portefeuille composé d'OAT dix ans, dont 10 % arrivent à échéance chaque année ; taux de réinvestissement à partir de 2015 égal à 0,55 % (niveau de l'OAT dix ans au 30 janvier 2015).

Sources : Banque de France, Moody's Investors Service.

En effet, pour les assureurs dommages, la baisse des taux se traduit essentiellement par une baisse du résultat financier (4). Mais celui-ci reste normalement positif, et cette baisse peut en théorie être compensée par une amélioration du résultat technique, par exemple au travers de majorations tarifaires.

Les assureurs vie, quant à eux, ont le plus souvent offert des taux garantis à leurs assurés. Lorsque le rendement des actifs diminue, il y a alors un risque

que ce rendement devienne inférieur au taux garanti. Dans ce cas, l'assureur vie enregistre des pertes, et sa solvabilité se détériore. Par ailleurs, comme l'assurance vie est par nature une activité de long terme, il y a peu de possibilité de corriger rapidement la situation lorsque les problèmes surviennent, contrairement à l'assurance dommages où la tarification peut en général être revue chaque année et les dérives rapidement corrigées, une fois identifiées. Dans la suite de cet article, nous nous concentrerons sur les assureurs vie.

L'impact négatif de la baisse des taux d'intérêt n'est généralement pas visible immédiatement dans les comptes ou dans les ratios actuels de solvabilité réglementaire (Solvabilité I). Paradoxalement, la baisse des taux peut même apparaître de façon positive. Ainsi, une baisse des taux augmente la valeur de marché des actifs obligataires, ce qui se traduit par une augmentation des fonds propres en normes IFRS (où les actifs sont valorisés en valeur de marché, tandis que les passifs sont pour l'instant évalués selon les normes locales, c'est-à-dire, dans la grande majorité des cas, qu'ils ne sont pas valorisés en valeur de marché) ; ce qui se traduit également par une augmentation des ratios de solvabilité dans certains pays comme la France, où les plus-values obligataires font partie des éléments constitutifs de la marge de solvabilité (tandis que le besoin de marge n'est fonction que de la valeur des provisions, qui ne dépend en général pas de l'évolution des taux d'intérêt).

Le véritable impact de la baisse des taux d'intérêt apparaît le plus souvent tardivement dans les comptes. Un certain nombre d'assureurs ont par exemple déprécié dans leurs comptes IFRS une partie de leurs actifs intangibles (écarts d'acquisition ou frais d'acquisition reportés notamment), mais de futures dépréciations ne sont pas à exclure car les hypothèses utilisées pour l'évaluation de ces actifs sont parfois optimistes au regard des taux d'intérêt actuels.

Certaines juridictions ont également introduit en normes locales des provisions pour permettre aux assureurs de faire face à une partie du risque lié à la baisse des rendements financiers (provision pour aléas financiers en France, ou Zinszusatzreserve introduite en 2011 en Allemagne). La constitution de ces provisions a un impact négatif sur le résultat des assureurs, mais cet impact ne traduit que partiellement le risque économique.

C'est pourquoi, dans sa méthodologie de notation des sociétés d'assurance, Moody's se réfère également à des indicateurs tels que la valeur intrinsèque (« *embedded value* ») ou les ratios de capital économique, qui sont plus à même de refléter l'impact réel d'une baisse des taux d'intérêt pour les assureurs vie (en supposant que cette baisse soit durable et non passagère). Les ratios Solvabilité II, qui tendent à se rapprocher des ratios de capital économique, reflèteront aussi de façon plus réaliste le risque lié aux taux d'intérêt pour l'ensemble des assureurs vie européens. Les stress tests menés par l'EIOPA l'année dernière ont révélé qu'en moyenne, sur la base des données financières à fin 2013, les assureurs vie perdraient environ 10 % de leurs fonds propres éligibles sous Solvabilité II dans un scénario de taux « à la japonaise ». Ils permettent ainsi de fournir une première évaluation de l'ampleur de la dégradation de la solidité financière des assureurs européens depuis fin 2013, puisque les taux ont atteint un niveau légèrement plus bas que celui retenu par l'EIOPA dans son scénario de stress (cf. supra).

L'exposition des assureurs varie selon le pays

Toutefois, l'exposition au risque de taux d'intérêt varie grandement d'un assureur à l'autre. Le risque est fonction du taux moyen garanti aux assurés (plus le taux garanti est élevé, plus le risque que le rendement des actifs devienne inférieur au taux garanti est élevé), mais surtout de l'écart entre la duration de l'actif et celle du passif. En effet, lorsqu'un assureur investit sur des actifs plus « courts » que ses passifs, il doit réinvestir ses actifs avant que ses passifs arrivent à échéance. Si l'assureur a promis des taux élevés et que

les taux d'intérêt ont baissé depuis la souscription des engagements, l'assureur risque de réinvestir à un taux qui ne lui permettra pas de faire face à la garantie donnée. A contrario, si l'assureur a investi sur des actifs de même échéance que ses passifs, il ne supporte pas de risque de réinvestissement, et n'aura pas de difficulté à faire face à ses engagements (à condition que le taux garanti soit en adéquation avec les taux de rendement des actifs disponibles sur le marché au moment de la souscription des engagements).

Le taux moyen garanti varie d'un pays à l'autre, mais il est très similaire d'un assureur à l'autre au sein d'un même pays. Il reflète simplement les pratiques de marché dans chacun des pays. L'écart de duration peut être plus variable d'un assureur à l'autre, mais il existe tout de même de grandes similitudes au sein d'un même pays. L'écart de duration reflète en effet la nature et la duration des produits commercialisés (dans les pays où les contrats sont de très long terme, l'écart de duration est en général plus élevé car il est plus difficile de trouver des actifs de très long terme). Mais il reflète aussi les réglementations et les régimes comptables en vigueur dans chacun des pays (les écarts de duration sont généralement plus faibles dans les juridictions qui ont depuis longtemps pénalisé les écarts de duration, soit au travers de provisions spécifiques, soit au travers de comptabilisation des passifs en valeur de marché, soit au travers de réglementations spécifiques).

Le tableau 1 résume les caractéristiques des principaux marchés européens et les conclusions que Moody's en tire en termes d'exposition de ces différents marchés au risque lié à un environnement de taux durablement bas.

Tableau 1 : Exposition des assureurs vie au risque lié à un environnement de taux durablement bas dans les principaux marchés européens

	Espagne	France	Italie	Suisse	Norvège	Pays-Bas	Allemagne
% de produits garantis dans le bilan*	88 %	84 %	79 %	92 %	88 %	60 %	92 %
Taux moyen garanti sur les encours	variable	~1 %	2 % à 3 %	2 % à 3 %	3 % à 3,5 %	3,5% à 4 %	3 % à 3,5 %
Capacité à réduire les taux servis aux assurés	faible	de moyenne à élevée	moyenne	faible	moyenne	faible	de faible à moyenne
Écart de duration**	~ 1 an	~ 5 ans	~ 1 an	n/a	n/a	~ 5 ans	~ 11 ans***
Exposition globale au risque lié à un environnement de taux bas (opinion Moody's)	●◐○○	●●○○	●●○○	●●●◐	●●●◐	●●●●	●●●●

* Données à fin 2012.
** Duration du passif moins duration de l'actif : plus l'écart de duration est élevé, plus le risque de réinvestissement est élevé.
*** Y compris l'assurance santé.

Sources : European Insurance and Occupational Pensions Authority (EIOPA), Insurance Europe, Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV), Associazione Nazionale fra le Imprese Assicuratrici (ANIA), De Nederlandsche Bank (DNB), données publiées par les principaux groupes d'assurance européens, Moody's Investors Service.

Ainsi, la solidité financière des assureurs vie allemands est très susceptible de se dégrader fortement si les taux d'intérêt ne remontent pas, compte tenu du fort écart de duration entre leurs actifs et leurs passifs et du taux moyen garanti élevé promis aux assurés. Toutefois, il convient de noter que le marché allemand est très fragmenté : il existe de fortes disparités, les gros assureurs ayant en général une gestion actif-passif plus sophistiquée et un écart de duration plus faible que la moyenne du marché.

Les assureurs vie néerlandais sont également fortement exposés en raison d'un taux moyen garanti élevé, l'un des plus élevés en Europe.

Les pays scandinaves, et notamment la Norvège, présentent un profil assez similaire à celui de l'Allemagne, avec des taux garantis élevés et des écarts de duration entre actif et passif très élevés. Dans le cas de la Norvège, les taux d'intérêt sont toutefois légèrement plus élevés qu'en zone euro, ce qui laisse une marge plus confortable aux assureurs, du moins à l'heure actuelle.

De l'autre côté du spectre se trouve l'Espagne, où l'adéquation entre l'actif et le passif est une partie intégrante de l'essentiel des produits commercialisés. Le risque de réinvestissement est donc très faible. En Italie, les contrats d'assurance vie ont une duration relativement faible (de l'ordre de six ou sept ans, l'une des plus faibles en Europe), et l'adéquation entre l'actif et le passif est donc en général relativement aisée. Il en résulte là aussi un risque assez faible dans un environnement de taux bas, à condition que les nouveaux contrats commercialisés ne promettent pas de garantie extravagante au regard des conditions de marché.

Sur le marché français de l'assurance vie, le risque est aussi relativement limité en période de taux bas. En effet, même si l'écart de duration entre l'actif et le passif est plus élevé que dans d'autres pays, le taux moyen garanti est l'un des plus bas en Europe, et le risque de ne pas être en mesure de faire face aux garanties est donc faible. En réalité, un scénario de hausse brutale des taux d'intérêt serait plus dévastateur pour les assureurs vie français qu'un environnement de taux durablement bas, ce qui peut aussi expliquer pourquoi les assureurs français n'ont pas intérêt à augmenter trop significativement la duration de leurs actifs.

Les assureurs français pâtissent tout de même de la baisse des taux d'intérêt, notamment au travers d'une baisse des résultats financiers. Toutefois, s'ils continuent d'agir de façon rationnelle, c'est-à-dire s'ils continuent de baisser les taux servis aux assurés et de ne pas distribuer plus que ce qu'ils génèrent, ils devraient rester en mesure de protéger leur solvabilité. Le défi principal pour les assureurs français dans un environnement de taux bas reste de trouver le bon équilibre entre le maintien de leur solidité financière et le maintien de l'attractivité de leurs produits (cf. infra).

Les assureurs tentent de préserver leur solidité financière

Dans tous les pays européens, les assureurs utilisent les mêmes recettes pour contrer les effets de la baisse des taux d'intérêt. Tout d'abord, ils baissent les taux servis aux assurés de façon à partager les effets de la baisse des rendements financiers avec les assurés. Toutefois, dans les pays où les taux moyens garantis sont élevés, cette stratégie est de plus en plus limitée, car les assureurs ne peuvent pas servir moins que la garantie.

Ils modifient également les nouveaux produits qu'ils commercialisent, soit en baissant les taux garantis, soit en privilégiant la commercialisation des contrats en unités de compte, sans garantie. Une palette de produits intermédiaires ou hybrides (comme les contrats eurocroissance en France) se développe également. Ces produits ne garantissent qu'une partie de l'épargne ou n'offrent des garanties qu'à l'échéance des contrats (en opposition aux garanties annuelles typiquement données par les assureurs dans la plupart des pays européens). La commercialisation

et l'accumulation au bilan de ces produits moins risqués (pour l'assureur) aura au fil du temps un impact positif sur le profil de risque des assureurs.

Toutefois, la nouvelle production reste relativement faible par rapport au stock de contrats existants, et de nombreuses années seront donc nécessaires pour que ces mesures portent leurs fruits. Par ailleurs, la baisse des taux servis et/ou des garanties réduit inévitablement l'attractivité des produits d'assurance. Même s'il est peu probable qu'apparaissent des produits de substitution avec des niveaux de garantie équivalents à ceux auxquels s'étaient habitués les clients, il faudra du temps pour convaincre les consommateurs de changer leurs habitudes et de souscrire massivement à des produits sans garantie. On peut donc s'attendre à court terme à une baisse de la production des assureurs, ce qui réduit d'autant l'impact positif attendu de la nouvelle production sur le profil de risque des assureurs. Notons aussi que, dans une volonté extrême de réduire les garanties, les assureurs s'exposent à une plus grande concurrence directe avec les gérants d'actifs. Le spectre des compétiteurs s'élargissant ainsi, les marges des assureurs vie vont aussi diminuer.

En parallèle, les assureurs vie développent leurs activités de prévoyance et de santé. Toutefois, dans le contexte économique actuel, il est difficile de commercialiser des produits non obligatoires, et si ces produits génèrent en général des marges plus attractives que les produits d'épargne, les volumes devraient rester faibles.

Enfin, les assureurs modifient leur allocation d'actifs, à la recherche de rendement supplémentaire. Compte tenu de la faiblesse des taux d'intérêt, des opportunités créées par la désintermédiation croissante de l'économie, mais aussi après prise en compte des contraintes imposées par la future réglementation Solvabilité II, les assureurs devraient investir de plus en plus (jusqu'à 20-30 % de leur bilan à long terme) sur des actifs illiquides : prêts aux entreprises (comme cela se développe en France), prêts infrastructure (comme au Royaume-Uni ou en Allemagne), prêts immobiliers (comme aux Pays-Bas) ou investissements directs dans l'immobilier.

Même si les actifs illiquides ne sont pas nécessairement plus risqués que les autres classes d'actifs, il est important de souligner que les assureurs sont novices sur ces actifs et ne possèdent pas tous une grande expertise dans ce domaine. Il leur sera donc difficile de ne sélectionner que les meilleurs actifs illiquides. Puisque les actifs illiquides remplaceront les actifs les moins rémunérateurs pour les assureurs, qui sont en général également les moins risqués, il est très probable que la qualité globale des actifs des assureurs diminuera progressivement.

Cette conséquence indirecte de la baisse des taux d'intérêt contribuera également à affaiblir la qualité de crédit des assureurs européens.

Notes

1. Le 15 janvier 2015, la Banque nationale suisse a mis fin au taux plancher de 1 euro pour 1,20 franc suisse et a décidé de baisser ses principaux taux directeurs. Le 19 janvier 2015, la Banque nationale du Danemark a également annoncé une baisse de ses taux directeurs.

2. À l'exception du Royaume-Uni où les taux sont plus élevés et sont attendus en hausse à moyen terme.

3. OAT : obligations assimilables du Trésor. Les OAT sont les obligations émises par l'État français.

4. La baisse des taux peut aussi impacter le provisionnement des assureurs dommages. Par exemple, l'évaluation des provisions mathématiques de rente automobile en France ou au Royaume-Uni (connues sous le nom de Periodic Payment Order *ou PPO) est sensible au niveau des taux d'intérêt, et une baisse des taux peut se traduire par une augmentation des provisions. Ce sujet ne sera toutefois pas abordé dans cet article.*

La genèse d'une innovation l'eurocroissance

Stéphane Dedeyan

Directeur général délégué, Generali France

Président des commissions plénières assurances de personnes de l'Association française de l'assurance (AFA) et de la Fédération française des sociétés d'assurance (FFSA)

Fruit de deux ans de travail entre les assureurs et les pouvoirs publics, l'eurocroissance donne un nouveau cadre technique à l'assurance vie. Ce cadre devrait permettre au placement préféré des Français d'affronter dans la durée un environnement de taux bas radicalement nouveau. Il devrait également renforcer sa capacité à financer l'économie, tout en améliorant les perspectives de rendement pour l'épargnant. Le processus d'élaboration de cette construction technique nouvelle, dans le dialogue avec les pouvoirs publics et la recherche permanente de l'alignement des intérêts de toutes les parties prenantes, pourrait servir d'exemple à bien des réformes. Lancé depuis la fin 2014, l'eurocroissance nécessite maintenant des efforts soutenus pour trouver progressivement sa place dans le paysage de l'assurance vie, et stimuler une prise de risque graduelle dans les comportements des épargnants français.

L'assurance vie, levier de financement de la croissance

C'est sans aucun doute au dernier trimestre 2012 que tout commence. Et c'est Louis Gallois qui pose la première pierre de la construction de l'eurocroissance. Dans son diagnostic structurel des causes du décrochage de l'industrie française [2012], il distingue nettement deux blocs de causes. D'une part, la nécessité de redynamiser la recherche et l'innovation et de mieux les articuler avec l'industrie. D'autre part, une orientation insuffisante des flux de financement vers le tissu industriel. Les bases de toute la construction sont posées : pour relancer durablement la croissance, il faut privilégier l'investissement productif, l'investissement long, celui qui permet, par l'innovation, un rééquilibrage dans la durée de la compétitivité prix et hors prix. Qui dit investissement long dit épargne longue ; et donc, en France, l'assurance vie, avec ses 1 500 milliards d'euros d'encours.

C'est donc très logiquement que, dans le prolongement du rapport Gallois, le gouvernement demande au Parlement (1) de réfléchir aux moyens de réformer l'épargne financière, pour contribuer utilement à un meilleur financement de l'économie. Dans leur rapport, remis en avril 2013, les députés Karine Berger et Dominique Lefebvre mettent en avant deux objectifs. En premier lieu, consolider la confiance des épargnants pour favoriser une épargne longue. En second lieu, mieux inciter aux placements longs et risqués pour

répondre aux besoins de financement des entreprises de taille intermédiaire (ETI) et des petites et moyennes entreprises (PME). Afin d'atteindre ces objectifs, ils proposent notamment d'organiser une réorientation des encours de l'assurance vie vers les placements les plus ciblés sur le financement des entreprises, sans déstabiliser le produit. Le modèle de l'assurance vie était donc amené à évoluer.

Les ordres de grandeur de l'équation macroéconomique sont rappelés par les deux députés dans leur troisième recommandation. Il s'agit de « réorienter et mobiliser à hauteur de 15 à 25 Md€ par an et 100 Md€ d'ici la fin du quinquennat l'épargne financière des ménages en faveur des entreprises et plus spécifiquement des PME et des ETI ». Cet effort d'environ 100 Md€ se répartirait en trois : le Livret A, l'assurance vie, et le retour des investisseurs institutionnels vers le financement des PME en croissance et le capital investissement.

La recherche d'un alignement de tous les intérêts

De la fin d'année 2012 à l'automne 2014, un dialogue nourri entre les assureurs et les pouvoirs publics permettra de porter sur les fonts baptismaux une innovation majeure pour l'assurance vie, destinée à participer à cet effort : l'eurocroissance. Très vite, la question de la fiscalité est centrale. Faut-il pénaliser la fiscalité de l'assurance vie en euro afin d'orienter l'épargne longue des Français vers les supports les plus risqués, de type unités de compte ? Pour les assureurs, le risque de déstabiliser, par une action qui serait perçue comme rétroactive, l'ensemble de cette construction patiente, fondée sur la confiance, qu'est l'assurance vie est trop important. Il est vrai que, déjà à l'époque, les constats sont sans appel : une décroissance programmée des rendements des fonds euro du fait de la baisse des taux d'intérêt, une aversion au risque des épargnants plus élevée que jamais – en pleine crise des dettes souveraines – et une capacité pour les assureurs d'investir dans des actifs risqués limitée par la perspective des nouvelles règles Solvabilité II. Les difficultés objectives étaient suffisantes pour ne pas en ajouter une autre, qui aurait attaqué le cœur même de l'édifice en remettant en cause l'unicité et la simplicité des contrats.

Il fallait donc pour la profession être force de proposition. L'ampleur de l'effort demandé pour avoir un impact sur l'investissement et la croissance était telle qu'elle ne pouvait être atteinte qu'au travers d'un véritable avantage pour l'épargnant. Et il fallait que cet avantage puisse profiter non seulement aux nouveaux contrats et versements, mais aussi au stock de 1 500 Md€ d'encours. Il s'agissait donc de s'attaquer au cœur du problème : retrouver des perspectives de rendement à l'ensemble de l'assurance vie sans sacrifier la garantie en capital.

C'est un examen en profondeur de cette garantie du capital dans les fonds euro qui fournit la réponse. Celle-ci est accordée à tout instant. C'est extrêmement contraignant pour l'assureur, car cela l'oblige à investir massivement dans des supports obligataires. Et, avec la baisse des taux, cela pèse sur le rendement pour l'assuré. Compte tenu de l'aversion au risque des épargnants, il n'est pas question de supprimer cette garantie en capital. Il s'agit de ne l'accorder qu'à un certain terme, d'au moins huit ans, voire de quinze à vingt ans et plus pour des contrats retraite par exemple. Ce relâchement de contrainte et l'allongement de la durée de détention des contrats ainsi provoqué libèrent l'espace nécessaire pour des investissements plus risqués pour l'assureur. Et ces investissements sont générateurs de rendement pour les épargnants et de financement de l'économie productive pour les pouvoirs publics.

Les simulations effectuées par les principaux acteurs du marché de l'assurance vie, tant dans le cadre d'une approche rétrospective que dans le cadre d'une modélisation prospective, ont rapidement montré que l'espérance de rentabilité supplémentaire apportée par cette innovation était bien supérieure à celle d'un fonds euro classique. Sur une période de

détention suffisamment longue, plus de quinze ans par exemple, ce rendement supplémentaire est de l'ordre de + 1 % par an.

On peut ainsi offrir une véritable innovation, qui vient se placer entre l'assurance vie « euro » et l'assurance vie en « unités de compte ». Dans la première, l'assuré ne supporte aucun risque car elle lui offre une garantie en capital à tout moment, mais avec un rendement de plus en plus faible. Dans la seconde, l'espérance de rendement est supérieure, mais l'assuré supporte tout le risque ; il n'y a aucune garantie en capital. Et pour peu que ce mouvement puisse profiter à tous les contrats existants sans novation fiscale, c'est l'ensemble du stock de 1 500 Md€ qui sera éligible à la transformation. Toutes choses égales par ailleurs, en convertissant progressivement 15 % à 20 % de la part d'épargne assurance vie 100 % euro, soit un montant de l'ordre de 200 Md€, le financement en actifs risqués par les assureurs progresserait de 40 Md€ environ. Cela permettrait à l'assurance vie d'apporter sa contribution à l'enjeu des 100 Md€ identifié par les députés. La sortie par le haut est trouvée. Elle sera approuvée par Dominique Lefebvre et Karine Berger, qui la reprendront dans leur rapport et lui donneront son nom : eurocroissance.

Une construction technique ambitieuse

C'est le fruit d'un dialogue nourri entre les assureurs et le Trésor. Les assureurs se mobilisent rapidement à partir du printemps 2013, avec les équipes du Trésor, pour préciser techniquement les contours de ce nouveau produit. Nous ne partions pas de zéro. Les contrats dits « euro-diversifiés », qui utilisent des mécanismes similaires à ceux de l'eurocroissance, ont servi de base. Et, progressivement, deux axes forts se sont dessinés, qui ont amené au final à une construction radicalement nouvelle. D'une part, l'ambition forte de créer un cadre technique porteur d'innovations pour la ou les prochaines décennies. D'autre part, la recherche de simplicité maximale pour les assurés, sans sacrifier leur bonne information.

Il était important de construire un nouveau cadre technique, plus large que l'eurocroissance proprement dit, afin de donner à l'assurance vie les moyens d'affronter durablement un environnement de taux bas. Règlementairement, il est alors décidé de ne pas fixer la garantie en capital à 100 %, mais de pouvoir la faire varier de 0 % à 100 %. Cela ouvre pour le futur de multiples perspectives. Ainsi, par exemple, avec un terme minimum de huit ans et un niveau de capital garanti au terme pouvant varier entre 80 % et 100 %, au choix de l'épargnant, les capacités d'investissement dans les actifs plus risqués sont maximisées. Et une sécurité pour les assurés est préservée. Afin de garantir une information claire, seuls les supports offrant une garantie du capital à 100 % peuvent être appelés eurocroissance, les autres sont appelés fonds « croissance ».

L'engagement de l'assureur est par ailleurs divisé en deux parties. D'un côté, un montant représentatif de la garantie de l'assureur à terme, la provision mathématique (PM), actualisée à un taux plus élevé que dans un fonds euro traditionnel, ce qui est beaucoup plus favorable pour des investissements de long terme. De l'autre, un montant autorisant une diversification vers des actifs plus risqués, la provision technique de diversification (PTD). En face de l'ensemble de ces engagements, les actifs sont mutualisés dans un compte d'affectation spécifique, différent de celui des engagements en euro. Ils sont comptabilisés en valeur de marché et non en valeur nette comptable, ce qui est le cas des fonds euro.

Cette valorisation au prix de marché, plus volatile, peut être déstabilisante pour les épargnants habitués aux fonds euro. Une provision de lissage, dite provision collective de diversification différée (PCDD), est ajoutée pour parachever le dispositif. Elle permettra d'atténuer pour les épargnants les variations de valeur trop importantes certaines années, inhérentes à ce nouveau mode de valorisation. Elle participera

également, au côté d'autres dispositions techniques complémentaires, à protéger la mutualité de tout comportement individuel opportuniste.

Il a souvent été entendu que ce nouveau produit présentait pour l'assuré moins de liquidité qu'un fonds euro traditionnel. Cela est inexact. L'assuré peut, si les conditions générales du contrat le permettent, procéder à tout instant à des rachats. L'épargne est donc bien liquide. Le seul élément à préciser est que l'épargne est valorisée à sa valeur de marché tant que le terme n'est pas atteint. Et il faut attendre ce terme pour faire disparaître la volatilité.

Enfin, il fallait s'ouvrir au volume le plus large possible, avec le maximum de simplicité pour les épargnants. Ainsi, les fonds (euro)croissance peuvent être alimentés à la fois par la souscription de nouveaux contrats et par la conversion d'une partie des contrats en cours, sans que cela n'entraîne la perte des avantages fiscaux acquis. Cette conversion sera possible selon deux modalités. Premièrement, via l'ajout d'un fonds (euro)croissance dans les contrats multisupports de dernière génération. Deuxièmement, via la conversion des vieux contrats, en utilisant le mécanisme mis en place par la loi de modernisation de l'économie de 2005 (dispositif dit « Fourgous »). Ainsi, les anciens contrats monosupports euro et les contrats multisupports de première génération pourront être transformés en contrats de dernière génération. Le bénéfice pour l'assuré est important, car les contrats récents sont plus adaptés aux dernières tendances nées de la digitalisation : valeur des contrats consultable en ligne, actes de gestion en self-service via internet, etc.

Une innovation fondée sur l'intérêt général

Sur ces fondements techniques, issus d'un travail de plus d'un an et d'une collaboration rapprochée entre les services du Trésor et la profession, il peut être affirmé que l'ensemble des acteurs concernés par cette innovation sont gagnants :

- tout d'abord l'épargnant, qui verra, sur la durée, son épargne rapporter plus que dans un fonds euro traditionnel, sans abandonner toute garantie en capital ;

- les entreprises, et en particulier les ETI et PME, qui trouvent plus de financements. L'assureur n'étant plus tenu de garantir le capital à tout instant, il peut investir dans des actifs plus risqués, comme des actions, des titres de PME-ETI, du non coté ;

- l'État, qui peut mieux orienter l'assurance vie vers le financement productif. Les objectifs de politique publique sont favorisés, grâce à une modalité intelligente de mobilisation de l'épargne de tous les Français ;

- enfin les assureurs, qui peuvent préserver leur marge et leur solvabilité dans un contexte adverse. Pour un même niveau d'immobilisation du capital, leurs actifs procurent plus de rendement.

Un effort à poursuivre

L'objectif de l'eurocroissance est bien de provoquer un financement supplémentaire de l'économie en jouant sur le stock de fonds euro, pour le transformer progressivement et significativement. Son succès est donc important pour participer à la relance de l'économie.

Les réseaux commerciaux des assureurs vie sont aujourd'hui mobilisés, avec une volonté forte d'implication, exprimée par les plus gros acteurs du marché.

Les conditions historiquement basses de taux d'intérêt vont rendre la tâche plus difficile aux assureurs. Elles réduisent mécaniquement les capacités d'investissement dans des actifs plus risqués, générateurs de

rendements financiers dans la durée. Il est donc aujourd'hui plus que jamais nécessaire de poursuivre le dialogue avec le ministère des Finances et de soutenir fortement le lancement de l'eurocroissance.

Il faudra aussi laisser le temps aux professionnels de l'assurance de faire leur travail de conviction auprès des assurés, dans le respect du devoir de conseil lié à chaque situation particulière. Il ne s'agit pas de remplacer brutalement toute l'épargne euro par de l'épargne (euro)croissance. Il s'agit de mettre tout en œuvre pour convertir progressivement 15 % à 20 % des encours euro en (euro)croissance, en commençant par les épargnants qui ont le plus à y gagner. C'est-à-dire ceux qui sont investis à 100 % en fonds euro, sans pour autant avoir besoin, pour toute leur épargne assurance vie, d'une garantie de 100 % de leur capital à tout instant.

Ainsi, dans la durée, ce cadre technique nouveau qu'est l'eurocroissance permettra à l'assurance vie de se réformer en douceur, sans casser la confiance avec les épargnants, ce qui est fondamental. Et, en dernière analyse, c'est la progression de la part des encours eurocroissance et unités de compte dans les encours totaux de l'assurance vie qu'il faudra mesurer. L'objectif final est en effet de pouvoir mieux financer l'économie productrice, porteuse de croissance durable. Et cela passe notamment par une prise de risque globalement accrue dans le placement préféré des Français, sans le déstabiliser.

Note

1. Mission confiée aux députés Karine Berger et Dominique Lefebvre le 9 octobre 2012.

Bibliographie

BERGER K ; LEFEBVRE D., « Dynamiser l'épargne financière des ménages pour financer l'investissement et la compétitivité », rapport au Premier ministre, 2 avril 2013, Archives du ministère de l'Économie et des Finances.

GALLOIS L., « Pacte pour la compétitivité de l'industrie française », rapport au Premier ministre, 5 novembre 2012, La Documentation française.

L'EUROCROISSANCE L'INNOVATION DANS L'ASSURANCE VIE

Emmanuelle Laferrère

Chargée de mission auprès du directeur de l'actuariat France, BNP Paribas Cardif

Pierre de Villeneuve

Président-directeur général, BNP Paribas Cardif, membre de l'Institut des actuaires (IA)

Le contexte financier actuel nous oblige à nous interroger, nous les assureurs, sur la pertinence des garanties que nous offrons. Le fonds en euros ne peut plus être aujourd'hui la réponse universelle. Dans un contexte de taux bas susceptibles de durer et d'érosion des rendements de nos actifs, l'eurocroissance apparaît comme la meilleure réponse aux objectifs de placement long terme de nos assurés et il est de notre devoir de les encourager à passer du fonds en euros aux fonds eurocroissance. La transition entre ces deux natures d'engagements conditionne l'avenir de notre métier d'assureur. Elle doit s'opérer dès maintenant et tout doit être mis en œuvre pour la faciliter : les transferts de richesse dans des conditions équitables, à l'occasion des arbitrages entre les fonds en euros et les fonds eurocroissance, semblent à ce titre indispensables.

Modifier la nature des engagements en assurance vie

Nous sommes là devant une nécessité impérieuse. Produit phare du paysage de l'assurance vie français, le fonds en euros est plébiscité par les épargnants pour sa sécurité et sa liquidité. Mais le paradigme du fonds en euros n'est plus adapté à la situation économique actuelle et à l'évolution des besoins de nos assurés. La première motivation des souscripteurs d'assurance vie est aujourd'hui la retraite. 27 % d'entre eux [1] souhaitent se constituer un capital ou une rente pour faire face à l'inexorable baisse des pensions des régimes de retraite de base et complémentaires. Si l'on y ajoute les assurés qui souhaitent transmettre un capital et ceux qui souhaitent épargner en vue d'un projet précis, ce sont plus de la moitié des souscripteurs d'assurance vie qui ont des objectifs de placement long terme et pour lesquels le fonds en euros seul ne peut plus être une réponse satisfaisante.

La protection permanente du capital a un coût financier qui devient de plus en plus important : l'obligation pour les gérants d'actifs de limiter la part actions et de privilégier les obligations de court

ou moyen terme va progressivement brider les performances du fonds en euros. Il est désormais indispensable que nous, assureurs, adaptions la nature de nos garanties vis-à-vis de nos assurés si nous ne voulons pas risquer de décevoir, tôt ou tard, leurs principales attentes.

La bonne réponse pour des engagements long terme

C'est dans ce contexte que le monde de l'assurance vie a vu naître en 2014 une nouvelle génération d'engagements : les fonds eurocroissance. Ces fonds ne sont pas totalement nouveaux, ils sont en réalité une évolution des fonds diversifiés dont ils reprennent la mécanique : un capital garanti à une échéance donnée, avec au passif de la société d'assurance une provision mathématique représentative des engagements garantis et une provision de diversification correspondant aux engagements complémentaires sans valeur garantie. À cela s'ajoute une réserve collective intitulée « provision collective de diversification différée » (PCDD) destinée, un peu comme la provision pour participation aux bénéfices du fonds en euros, à atténuer les baisses exceptionnelles de performance.

Affranchis de la garantie en capital à tout moment, ces fonds nous offrent une plus grande liberté dans notre allocation d'actifs. Nous pouvons, grâce à l'allongement de la duration des passifs, investir dans des obligations plus longues et, surtout, nous pouvons augmenter significativement la part dédiée aux actifs risqués, permettant ainsi à nos assurés d'espérer de meilleures performances sur le long terme. Les montants investis ne sont certes pas garantis à tout moment, mais la plupart des contrats d'assurance vie proposent, en cas de décès de l'assuré avant l'échéance, des garanties planchers afin de sécuriser l'épargne transmise aux bénéficiaires.

Autre avantage non négligeable, les fonds eurocroissance sont moins gourmands en capital que le fonds en euros. Cela est d'autant plus vrai dans l'environnement Solvabilité II qui tend à réduire l'appétit des sociétés d'assurance vis-à-vis du risque de marché.

En complément à ces avantages, il est important de souligner qu'avec des actifs plus longs et plus risqués, la philosophie de l'eurocroissance est totalement cohérente avec la volonté des pouvoirs publics de développer de nouveaux leviers de croissance pour les entreprises françaises.

Les fonds eurocroissance apparaissent donc comme une réelle opportunité de proposer des engagements en parfaite adéquation avec les attentes de performance à moyen et long terme de nos assurés et l'environnement économique actuel de taux d'intérêt très bas. Ils se positionnent naturellement au sein des contrats multisupports entre la promesse de sécurité de plus en plus « court-termiste » du fonds en euros et l'espérance de performance sans garantie des UC.

Un excellent compromis rentabilité/risques

Une mécanique inédite au passif, une valorisation en valeur de marché à l'actif, un cantonnement comptable... Proposer ces nouveaux engagements aux assurés demande aux sociétés d'assurance une expertise et une technicité très spécifiques.

Du côté opérationnel, la mise en œuvre des fonds eurocroissance nécessite de repenser totalement les moteurs de gestion, de modifier les schémas comptables et les flux de données échangés entre leurs différents systèmes informatiques. Cela représente des coûts humains et de développement importants pour le monde de l'assurance vie.

Mais les impacts ne se limitent pas à l'aspect technique : une véritable expertise est nécessaire afin de calibrer le meilleur ratio rentabilité/risques et de

suivre quotidiennement l'actif de ces fonds. La création de nouveaux outils de gestion actif/passif est capitale : nouvelles méthodes de définition de l'allocation stratégique, suivi de la part actions en fonction de la provision de diversification (multiplicateur, corridor...), suivi dynamique de l'adossement actif/passif, stratégie de dotation/reprise à la PCDD... Chez BNP Paribas Cardif, nos équipes ont développé une palette de nouveaux outils spécifiques à la gestion d'actifs de l'eurocroissance. Nos gérants connaissent en temps réel leur « budget de risque » afin de pouvoir réajuster leur portefeuille rapidement si nécessaire. D'autres indicateurs spécifiques, tels que la *Value-at-Risk*, ont également été intégrés à ce nouveau tableau de bord et donnent à nos gérants une vision « risque extrême » de leur portefeuille d'actifs. Tous ces outils sont indispensables pour assurer une gestion maîtrisée de l'eurocroissance.

Enfin et surtout, c'est tout le modèle de communication de l'assurance vie qui doit être revu avec ces nouveaux fonds. Il n'est pas possible de communiquer sur l'eurocroissance comme on le fait sur le fonds en euros : les promesses et les risques sont différents, il faut à tout prix éviter les amalgames. Un important travail de pédagogie est nécessaire auprès des assurés, mais aussi des distributeurs, pour expliquer cette nouvelle mécanique : garantie au terme, évolution à la hausse ou à la baisse de la valeur du fonds en cours de vie, performance du fonds et performance individuelle… La méthode de communication sur la performance est un point fondamental pour la compréhension et la réussite des fonds eurocroissance. Il serait erroné de vouloir jouer le jeu de la comparabilité avec le rendement annuel du fonds en euros puisque les deux types d'engagements ne suivent pas les mêmes règles. Les assurés et les distributeurs doivent « oublier » la notion de taux servi et penser performance sur le long terme.

La compréhension de cette nouvelle logique de pensée n'est pas évidente, comme nous avons pu le constater depuis le lancement de notre premier contrat diversifié en 2010. Mais nous avons développé au fil des années un langage adapté et des outils spécifiques, tels que des reportings dédiés et commentés, afin de renforcer la communication autour de l'eurocroissance. Notre travail de pédagogie n'est pas terminé pour autant, et il est indispensable que tous les assureurs proposant ce type de fonds élaborent une communication propre à l'eurocroissance.

La nécessité d'engager la transition maintenant

Mais aujourd'hui certains doutent : une telle dépense d'argent et d'énergie pour lancer et gérer ces nouveaux fonds est-elle vraiment pertinente dans un environnement de taux bas ? Nous répondons oui ! Car la stratégie de l'eurocroissance est gagnante, particulièrement si la période de taux bas doit être durable.

Créé ex nihilo aujourd'hui, un fonds en euros ne serait pas viable. Face à un risque de marché extrêmement fort, le seul choix raisonnable pour un gérant d'actifs serait d'avoir une part actions proche de zéro et de n'investir que dans des obligations courtes (cinq ans maximum) afin de se couvrir contre le risque de hausse des taux. Avec un rendement autour de 1 % et après déduction des frais de l'assureur, le rendement pour les assurés serait quasi nul. Dans le contexte financier d'aujourd'hui, un fonds eurocroissance est plus efficient : avec un horizon de placement entre quinze et vingt ans autorisant une part actions représentant 25 % à 40 % de l'actif et l'achat d'obligations de moyen ou long terme, son espérance de rendement net serait supérieure d'au moins 100 points de base.

Certes, le fonds en euros sert des taux encore séduisants, mais l'érosion est bien en marche. En 2014, le rendement net moyen est estimé par la FFSA à 2,50 % (2), en baisse de 30 points de base par rapport à l'année précédente. À plus ou moins long terme, les obligations au sein du fonds en euros vont arriver à échéance et seront remplacées par des

obligations aux niveaux de taux actuels, laissant le rendement net du fonds en euros tendre doucement vers zéro. Mais n'attendons pas cette situation pour agir car il sera alors trop tard. Notre devoir est d'engager la transition entre le fonds en euros et les fonds eurocroissance, en encourageant dès aujourd'hui nos assurés à passer de l'un à l'autre.

Transfert de richesse : entre droit et nécessité

Si le fonds en euros affiche encore des rendements particulièrement intéressants, c'est parce qu'il bénéficie d'une « richesse » accumulée au fil du temps : provision pour participation aux bénéfices, titres en plus-value, obligations anciennes... Mais cette richesse ne doit pas conduire à privilégier l'actif le moins diversifié et freiner les arbitrages entre le fonds en euros et l'eurocroissance.

Nous, assureurs, avons des devoirs vis-à-vis de nos assurés, notamment l'obligation de leur conseiller toutes les adaptations contractuelles qui permettraient de mieux satisfaire leurs attentes. Aujourd'hui, il paraît légitime de considérer les assurés du fonds en euros et ceux de l'eurocroissance comme une même mutualité et d'encourager les arbitrages vers l'eurocroissance. Dans ce cadre, un transfert de richesse entre les deux fonds est tout à fait logique.

Rappelons au passage que la provision pour participation aux bénéfices « libre » provient souvent d'un sacrifice de marge concédé par l'assureur et que, dans ce cas a fortiori, ce dernier devrait être libre de l'affecter comme il l'entend pour mieux servir ses assurés, qu'ils aient fait le choix du fonds en euros ou de l'eurocroissance.

Tout transfert de richesse étant basé sur un principe d'équité entre deux grands types d'engagements gérés chacun de manière mutualisée, la richesse transférée à l'eurocroissance devrait être affectée à la provision collective de diversification différée (PCDD), sans droit individuel immédiat, à charge pour l'assureur de répartir cette réserve en cas de baisse de la valeur du fonds.

Un début prometteur

La transition a déjà démarré. BNP Paribas Cardif a vu en 2009, avec des taux de l'OAT dix ans inférieurs à 3,5 %, la nécessité d'exploiter les atouts des contrats diversifiés. Avec le lancement de notre premier contrat de ce type en octobre 2010, nous avons acquis une réelle expertise qui nous rend confiants pour l'avenir. Fin 2014, nos deux contrats phares rassemblaient 90 000 assurés et un encours de près d'un milliard d'euros, pour des performances annualisées depuis leur création de 6,05 % pour le premier contrat (entre octobre 2010 et décembre 2014) et de 8,92 % pour le second (entre avril 2012 et décembre 2014). Preuve qu'à ce stade, ce changement est une réussite pour les assurés qui nous ont fait confiance.

Notes

1. Enquête AFA 2014 auprès de 5 586 souscripteurs de nouveaux contrats d'assurance vie en cas de vie.

2. Source : conférence de presse FFSA du 29 janvier 2015.

Quelles stratégies de gestion ?

Éric Bertrand

Directeur adjoint des investissements

Directeur de la gestion de taux et de crédit

CPR Asset management

Arnaud Faller

Directeur des investissements, CPR Asset management

Président de la commission des techniques de gestion

Association française de la gestion financière (AFG)

Les taux sont bas, historiquement, économiquement, financièrement. La réponse non conventionnelle des banques centrales à la double crise que nous avons connue (subprimes *puis eurozone), si elle a permis d'éviter une répétition des années 1930, nous amène aujourd'hui en* terra incognita.

Plus que jamais, il est aujourd'hui difficile de gérer la matière obligataire dans ce contexte où la rémunération du passage du temps par le coupon est remise en cause. Nous proposons ici quatre approches différentes qui nous apparaissent pertinentes, tant dans la philosophie de gestion que dans la stratégie d'investissement :

- *tout d'abord la diversification des investissements, même si beaucoup de champs ont été ouverts récemment, il en reste encore de nombreux à intégrer ;*
- *la flexibilité, qui certes est un challenge dans un cadre contraint mais va devenir cruciale dans les années à venir ;*
- *les investissements en devises étrangères, une partie de la réponse européenne aux taux bas se trouve en dehors de la zone d'investissement naturelle ;*
- *et enfin, des stratégies de gestion qui permettent de retrouver du gain au passage du temps.*

0,48 %, c'est aujourd'hui le taux de rendement médian des quelque 11 500 milliards de dette obligataire en zone euro, tous émetteurs et notations confondus. Si on se restreint à la dette de catégorie investissement de moins de dix ans, ce taux médian atteint 0,31 %. Clairement les taux sont bas ; pis, 25 % de toute la dette souveraine des États de la zone euro est en taux négatifs (cf. tableau ci-dessous). Prêter de l'argent coûte désormais cher. Le risque associé n'a pas pour autant disparu, que ce soit en duration ou en qualité de crédit des emprunteurs. On est progressivement passé du taux sans risque au risque sans taux.

Cartographie des émetteurs de la zone euro à fin janvier 2015

	< 0	0 << 1	1 << 2	> 2	MEDIAN
Total	15 %	59 %	17 %	9 %	0,48
	< 0	0 << 1	1 << 2	> 2	MEDIAN
Inférieur à 5 ans	32 %	61 %	4 %	4 %	0,18
5 - 10 ans	3 %	67 %	24 %	6 %	0,53
Supérieur à 10 ans		42 %	34 %	24 %	1,12
	< 0	0 << 1	1 << 2	> 2	MEDIAN
AAA-AA-A	23 %	68 %	9 %	0 %	0,25
BBB		47 %	34 %	18 %	1,06
HY		9 %	27 %	64 %	2,50

Comment en est-on arrivé là ?

Dans l'onde de choc postcrise de 2008, la Banque centrale américaine a réalisé que le désempilement des bilans bancaires ainsi que les pertes associées ne sauraient être contenus avec les mesures classiques de politique monétaire que sont les baisses de taux directeurs. La Fed s'est donc massivement mise à acheter des titres sur le marché obligataire, afin d'éviter des réactions en chaîne après les faillites de Lehman, Washington Mutual, AIG... et d'écarter un risque systémique d'implosion des marchés financiers. Son bilan s'est ainsi dilaté de près de 3 000 milliards de dollars, soit près de 25 % du PIB des États-Unis. Certes, dans le même temps, le besoin de financement de l'État américain s'est accru de quelque 1 200 milliards de dollars, mais au total c'est bien 1 800 milliards de dollars qui se sont investis sur le marché obligataire avec la duration qui y est associée.

Depuis, les banques centrales d'Angleterre, du Japon et, tout récemment, la BCE se sont également lancées dans des programmes majeurs d'achats de titres, le fameux assouplissement quantitatif (en anglais *quantitative easing, QE*). L'ensemble des achats ainsi effectués par les banques centrales s'élève à plus de 7 000 milliards de dollars, près de 20 % du PIB de ces quatre zones. Ces mesures, outre leur aspect antirisque systémique, ont aussi pour but de pousser les investisseurs à se délester de leurs actifs obligataires, majoritairement souverains, ne rapportant quasiment plus rien, pour aller vers des actifs plus risqués (crédit et actions) et favoriser ainsi le redémarrage de l'économie. Sachant que, dans le même temps, de façon assez contradictoire, la réglementation se durcit pour les intervenants de marchés (Bâle III pour les banques, Solvabilité II pour les assureurs ...), ne les encourageant pas spécialement à reprendre du risque.

Le risque, en cas d'ajustement économique ou budgétaire trop violent, d'absence de confiance des investisseurs et donc de faible demande de crédit ou d'investissement productif, est d'aboutir à une sorte de trappe à liquidité qui entraîne les taux à un niveau très bas pour très longtemps, sans pour autant favoriser le redémarrage de l'économie.

Historiquement, les crises d'endettement passent souvent par deux voire trois des phases suivantes : une phase de baisse des valeurs des actifs entraînant des vagues de défauts des banques ou des émetteurs souverains (Lehman et consorts dans la crise des *subprimes*, la Grèce dans la crise de la zone euro) ; puis une phase de répression financière où les acteurs se retrouvent contraints de détenir des créances sans être rémunérés pour le risque porté ; enfin, une troisième phase d'inflation qui reste, en définitive, l'un des meilleurs moyens de se désendetter, notamment en coût politique, dans la durée, fût-ce au prix d'un transfert générationnel de richesses.

Nous sommes aujourd'hui dans une forme de deuxième phase, d'une façon plus ou moins contrôlée et souhaitée par la puissance publique. Les niveaux de

taux se sont depuis longtemps déconnectés des fondamentaux économiques habituels, croissance, inflation (encore plus aux États-Unis qu'en zone euro) et, même si l'exemple récent de la Suisse n'est pas généralisable, rien ne prouve que le point bas soit atteint. Partant de ce niveau, deux voies se dessinent à l'horizon des prochaines années :

• un cycle vertueux, entraîné par une économie américaine croissant à son potentiel, voire au-delà, qui se transmet au reste de l'économie mondiale, apportant un retour de la confiance et donc de l'investissement, ainsi qu'un peu d'inflation. Dans ce contexte, les taux seraient appelés à remonter, probablement très progressivement, sous la houlette des banques centrales qui ne voudraient pas voir un krach obligataire provoquer une violente rechute d'une économie convalescente ;

• ou bien, sous le poids des incertitudes économiques ou (géo)politiques, un cycle de déflation et de défiance généralisée qui se met en place avec un report des investissements, une charge de la dette grandissante au regard du PIB et des rendements toujours plus bas.

Dans ce contexte, vers quels investissements se tourner ? L'exemple des investisseurs japonais sur les dernières décennies est instructif. En effet, ceux-ci, partant d'une base très majoritairement nationale, ont dû s'adapter. La chasse au rendement les a poussés dans un premier temps vers des investissements toujours plus loin sur la courbe, puis sur les ratings ; et, dans un second temps, sous l'effet d'éviction produit par les achats de la Banque centrale, vers des investissements en devises étrangères d'abord couverts puis en acceptant le risque de change.

Dans le moment présent, ces forces sont déjà à l'œuvre et devraient s'accentuer compte tenu de l'ampleur des programmes d'assouplissement quantitatif. Cela dit, toute solution de recherche de rendement doit s'accompagner d'une analyse de risque associée : si la rémunération du risque a globalement diminué, il est essentiel de se concentrer sur les secteurs où elle reste la plus élevée en relatif et éviter le « mauvais » risque, c'est-à-dire le risque non rémunéré. De par le rendement très faible offert et le risque désormais asymétrique sur le niveau des taux, les anciennes stratégies de *buy and hold* ne sont plus pertinentes. De même, les gestions benchmarkées obligataires doivent être revues, car la sensibilité des indices est très forte au moment où la plupart des taux sont inférieurs à 1 % pour les maturités moyennes.

Plus globalement, les excellentes performances engrangées ces dernières années sur les actifs obligataires ne doivent pas faire perdre de vue la faiblesse des rendements à venir. Une obligation à 110 % de cours ne sera jamais remboursée qu'au pair ! Ce point, qui paraît trivial, est en général souvent occulté dans des investissements obligataires réalisés via des benchmarks ou des ETF, et pour lesquels l'approche par le taux de rendement est souvent reléguée au second plan et peu suivie.

Quatre stratégies pertinentes

Il nous semble que quatre grandes stratégies pertinentes en termes de performance ajustée du risque peuvent être mises en place : la diversification, la flexibilité, les investissements en devises et les stratégies optionnelles de portage.

La diversification

Après la crise des dettes souveraines, les obligations de dette privée ont pris une part quasi équivalente, voire supérieure, à celle des dettes gouvernementales dans les portefeuilles des investisseurs institutionnels. Avec la politique très volontariste de la BCE, notamment son assouplissement quantitatif, qui va quasiment « assécher » les émissions nettes de dettes d'État jusqu'en septembre 2016 au moins, il nous semble que les obligations privées cotées seront toujours très recherchées. Le taux de défaut des entreprises restera le premier critère, aussi bien pour celles situées dans la catégorie bien notée (*investment grade*) que pour celles situées dans le « haut rendement ». À ce jour, le

premier s'élève à moins de 0,5 %, alors que le second est à 2,5 % selon les anticipations des agences pour 2015, bien loin de la moyenne historique.

Il est intéressant de noter que la directive CRA (Credit Rating Agency), qui vise à une certaine « désintoxication » des agences, va entraîner une montée en puissance de l'analyse interne réalisée par les sociétés de gestion, et le poids du haut rendement de « qualité » devrait monter dans un grand nombre de portefeuilles.

Il nous semble qu'à côté de ce socle d'obligations privées, le poids des actifs de diversification va progresser, que ce soient les obligations privées, la dette infrastructure ou les prêts. Les réglementations semblent s'ouvrir petit à petit à ces classes d'actifs. Elles ont le double avantage d'offrir des émetteurs non forcément présents sur les obligations cotées, notamment par la taille de la société, et d'offrir une prime due à l'absence de liquidité permettant un surcroît de rendement en conséquence. En revanche, la quasi-impossibilité de revendre ces produits avant leur terme nécessitera une analyse poussée des risques portant sur les actifs investis. Mais il faut noter que le mouvement devra être assez long puisque l'offre de papier n'est pas à la hauteur de la demande : la moyenne du poids actuel au sein des sociétés d'assurance est entre 1 et 2 % de la totalité des investissements ; ces investissements ne peuvent donc être la seule solution pour résoudre la problématique d'investissement en période de taux durablement bas.

Une vraie alternative pourrait venir du côté des actions, sous réserve bien sûr du niveau des bénéfices délivrés par les sociétés et du niveau des valorisations des marchés actions. Il est intéressant de noter que l'écart entre le rendement délivré par les obligations *investment grade* et celui délivrés par les actions est quasiment au plus haut (1,5 % côté obligations taux et 3,5 % côté actions). Il nous semble que les investissements en actions pilotés dans un cadre de risque maîtrisé devraient voir leur part augmenter.

Nous avons bien conscience du frein créé par la réglementation (Solvabilité II ou Bâle III) et, de manière générale, par la crainte de revivre des scénarios catastrophes à l'image de 2008. Une manière de répondre est de proposer des stratégies actions protégées contre le risque extrême, en l'occurrence via des stratégies optionnelles. L'idée est de bien capter le potentiel des marchés actions mais de se protéger contre toute baisse excessive, par exemple au-delà de 15 % ou 20 %, via des *puts*. La gestion de ces stratégies optionnelles peut être soit systématique soit discrétionnaire, pilotée de manière très active pour optimiser le coût de couverture inhérent aux achats d'options. Pour fixer l'ordre de grandeur, nous pouvons estimer le coût de couverture de 3 à 5 % par an, qu'il est possible de réduire via des stratégies tactiques (à portage positif) pour le ramener de 2 à 3 %, voire moins.

Bien évidemment, cela suppose une bonne adéquation entre les positions détenues au bilan et celles du hors bilan pour que la couverture soit efficace financièrement (et reconnue par les autorités de régulation s'il s'agit de limiter le coût en fonds propres des investissements actions).

La flexibilité

L'une des conséquences de la faiblesse généralisée des taux est la réduction progressive du coussin de protection que représente le rendement récurrent d'une obligation qui permet d'absorber les aléas de la valeur de marché. En effet, de faibles variations de taux, et leur impact prix, viennent rapidement annuler la performance du coupon sur une année (0,06 % de hausse de taux sur une OAT dix ans avec un taux actuariel de 0,59 %). Cela conduit à considérer toute performance obligataire non seulement du point de vue de l'acquis, mais aussi du potentiel restant à percevoir ; et donc, en matière de gestion, de progressivement passer d'une approche très *buy and hold* à davantage de flexibilité. Certes une grande partie, par construction et contraintes réglementaire et comptable, restera sous ce format, mais il paraît opportun de déléguer une part à une gestion plus flexible permettant notamment d'encaisser les

gains réalisés sur des actifs obligataires, en particulier lorsque ceux-ci intègrent la majeure partie du rendement à venir.

Une approche flexible se confronte souvent à des problèmes de liquidité, de délais de réaction et de risque spécifique. Dans ce style de gestion flexible, il nous paraît opportun de privilégier une approche *top-down* par allocation de bêtas sur des compartiments de marché pour réduire ces risques en utilisant des supports d'investissements de type indices en physique ou via dérivés.

Sur le crédit notamment, en marge des investissements en titres directs, avoir une poche de gestion flexible allouée par grande catégorie de bêta nous paraît pertinent (IG *vs* HY, Euro *vs* US, Corp *vs* Fin...) en utilisant des supports indices diversifiés comme les *swaps* sur indices iTraxx (indice basé sur des *spreads* de dérivés de crédit, CDS) ou les TRS (*Total Return Swap*) sur les indices iBoxx (indices de titres de crédit physiques). Ces supports permettent des interventions rapides et assez significatives sur les marchés quand une opportunité se présente et, en raison de leur grande diversification, réduisent significativement le risque spécifique.

En outre, dans le cas du haut rendement, où l'attractivité du rendement se heurte souvent au risque spécifique lors de détention en titres vifs, l'approche via indice est intéressante. En effet, un défaut d'un émetteur n'est plus perçu comme une perte sèche sur une ligne en portefeuille (sur laquelle la communication est bien plus préoccupante que l'impact réel, et dont le poids est souvent supérieur à la granularité nécessaire pour pouvoir appliquer les tables statistiques de taux de défaut) ; mais il peut être appréhendé comme une hausse du *spread* moyen à l'échelle de l'indice, et donc être compensé par la performance globale de la classe d'actif.

Les investissements en devises

Les investisseurs institutionnels n'ont que rarement acheté des obligations en devises autres que l'euro. De plus, dans ces rares cas, la « position naturelle » était de les couvrir contre le risque de change ; la fameuse règle de congruence actif/passif du Code des assurances était mise en avant pour limiter les investissements en devises, y compris les placements actions internationales. La directive Solvabilité II modifie la donne, en considérant le change comme un facteur de risque comme les autres et fixant le choc à 25 %, niveau d'ailleurs identique au choc de l'immobilier physique.

Les politiques non conventionnelles des quatre grandes banques centrales ont évidemment bouleversé les marchés obligataires, mais aussi les marchés de change : la BOJ (et le gouvernement japonais) ont ainsi explicitement avoué avoir un objectif de dépréciation du yen alors que la BCE voit d'un bon œil, voire favorise, la dépréciation continue de l'euro ; le yen s'est déprécié de plus de 20 % par rapport au dollar depuis le 1er janvier 2014, et l'euro de 15 % depuis l'été 2014.

Il nous semble qu'adopter des positions stratégiques sur le dollar, que ce soit en actions, en obligations, en OPC monétaires, ou même en change à terme, a beaucoup de sens, en accompagnement des politiques annoncées pour plusieurs semestres par les banques centrales, et pour bénéficier de l'accroissement du bilan de la BCE (et de la stabilisation avant la décrue de celui de la Fed). L'action à la baisse de l'euro par la BCE pouvant de surcroît se coupler à un probable resserrement monétaire de la Fed en 2015.

La nature de ces investissements s'éloigne beaucoup des stratégies haute fréquence utilisées par les fonds spéculatifs et vise des tendances de fond. Il peut être également pertinent d'investir en obligations américaines et d'abandonner une petite partie du surrendement par rapport à son équivalent euro pour se couvrir, via le marché des options de change, contre un risque de dépréciation du dollar. Globalement, ces investissements ont également l'avantage d'être très liquides pour des tailles considérables, au contraire de certains actifs de diversification évoqués plus hauts.

La baisse des taux obligataires américains depuis début 2014, survenue à l'inverse du consensus, a sans doute pour origine des flux d'investisseurs européens et asiatiques à la recherche de rendement sur des obligations très bien notées.

De même, les investissements obligataires dans les pays émergents en devises locales peuvent être pertinents, principalement pour des raisons de portage : les rendements sont souvent plus élevés que ceux issus de la zone euro, mais ils s'accompagnent également d'un risque plus élevé (notamment sur la devise) qu'il conviendra de bien analyser. L'intérêt des investisseurs a augmenté avec l'amélioration des finances publiques des États émergents, d'autant plus que celles des pays de la zone euro se dégradaient, notamment dans le cas des pays de l'Europe du Sud. La sélection du pays devient primordiale, d'autant plus que le choix des pays est large et discriminant. Cette classe d'actifs a l'avantage de présenter une corrélation assez faible avec les investissements en dettes européennes. La liquidité des investissements est à bien prendre en compte en amont, car les marchés de dette émergente semblent subir des flux assez « moutonniers » aussi bien à l'entrée qu'à la sortie. La stratégie de *buy and hold* n'est de nouveau pas forcément la mieux adaptée pour cette classe d'actif.

Retrouver du thêta positif

La faiblesse des rendements et en particulier les taux négatifs posent clairement la question de la gestion du thêta, le passage du temps sur la détention d'obligations devant rapporter de la production financière et non en détruire. Il est donc pertinent de regarder d'autres actifs qui ont une composante intrinsèque systématique de leur performance en fonction du passage du temps. C'est le cas notamment des options où le thêta traduit le rapport gain/perte sur la prime de l'option en fonction du rapprochement de son échéance. Plus le temps passe, plus la probabilité que l'actif sous-jacent d'une option atteigne son prix d'exercice diminue, plus la valeur de sa prime baisse.

Une façon donc de repasser en thêta positif se trouve dans des stratégies à base de ventes systématiques d'options de part et d'autre de la monnaie (ventes de *put* et de *call : strangle*) ayant pour avantage de rapporter de la valeur temps tant que les marchés restent dans des bornes de fluctuations. Cependant, ces positions créent de la position ouverte en cas de « saut » de marché, ce qui est très consommateur de risque et malgré tout incertain dans l'environnement actuel. C'est pourquoi nous préférons couvrir le risque aux limites en rachetant ces *strangles* sur des bornes plus larges. La stratégie complète optimale étant une vente simultanée de *call spread* et de *put spread* autour de la monnaie. Ces stratégies étant bornées en risque, elles ne sont pas très coûteuses en capital ; en outre, sur les périodes où il y a des sauts de marchés la stratégie est neutre, gagnant sur un côté ce qu'elle a perdu de l'autre. Certains actifs obligataires peuvent ainsi être enrichis (voire substitués) avec des rendements significatifs. De plus, avec le développement des indices de dérivés de crédit iTraxx et CDX, ces stratégies optionnelles ne sont pas seulement cantonnées aux taux d'intérêt basés sur les dettes souveraines (aujourd'hui principalement la dette allemande en Europe), elles peuvent également être développées sur le crédit *investment grade*, mais également et surtout sur le haut rendement.

Conclusion

Quelle que soit l'issue de la période que nous traversons actuellement, la recherche de rendement au niveau européen comme mondial va pousser à avoir des courbes plus plates et un écrasement des primes de risques d'autant plus fort qu'elles sont importantes (haut rendement, pays périphériques, émergents…). Il sera toujours essentiel de privilégier les meilleurs couples rendements/risques, en relatif, la quasi-disparition des rendements des actifs de meilleure qualité ayant largement bousculé l'échelle avec laquelle les marchés fonctionnent depuis longtemps. Les approches évoquées dans cet article permettent d'y répondre, en partie, et ont été conçues pour pouvoir s'adapter à cet avenir incertain.

S'ADAPTER À UN UNIVERS DE TAUX DURABLEMENT BAS

Fabrice Rossary, CFA

Directeur des investissements et membre du directoire, Scor Global Investments

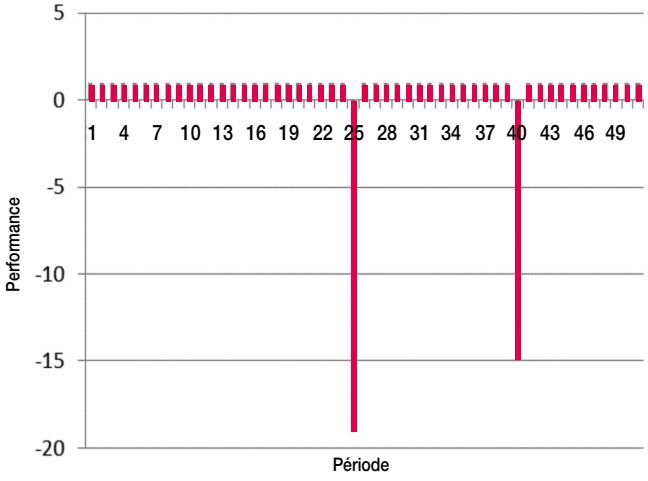
Les institutions ayant des engagements de long terme sont les premières impactées par l'univers de taux bas que nous connaissons, du fait notamment de la moindre rémunération de leurs placements. En effet, les trois grands types de stratégie qui sont à leur disposition en gestion d'actif voient leur efficacité fortement modifiée par le niveau faible des taux, le durcissement des règles prudentielles et l'application de normes comptables parfois inadaptées. Après une présentation succincte de ces stratégies et de leur utilisation par les investisseurs institutionnels, nous présenterons différents risques et techniques, dont la combinaison permet d'accroître le rendement récurrent d'un portefeuille, dans le cadre d'un environnement de contraintes du type de celles que rencontrent des investisseurs tels que les assureurs, et ce notamment dans la perspective de l'entrée en vigueur prochaine des normes Solvabilité II.

Stratégie d'investissement

Si l'on classe les stratégies d'investissement par typologie de génération de performance, nous pouvons trouver trois grandes familles :

• les stratégies de portage, où l'investissement est porté à son terme afin de bénéficier dans le temps d'une marge au-dessus du taux sans risque de même maturité, rémunérant un risque supplémentaire pouvant être de crédit, de liquidité ou de toute autre nature. Cette stratégie se caractérise par la très forte probabilité d'un gain limité et, inversement, par une très faible probabilité d'une perte totale ou quasi totale de l'investissement ;

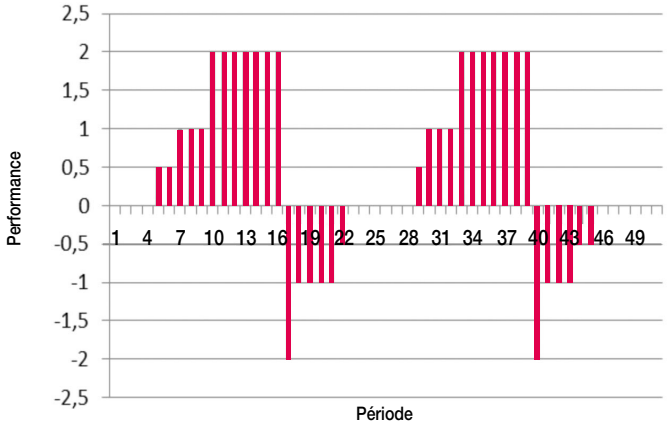
Figure 1 - Profil type d'une stratégie de portage : des rendements faibles mais très récurrents et des accidents isolés



Source : Scor Global Investments.

• les stratégies directionnelles, où l'investisseur cherche à tirer parti des tendances de marché en capturant l'accroissement ou la diminution du prix de l'actif sous-jacent ;

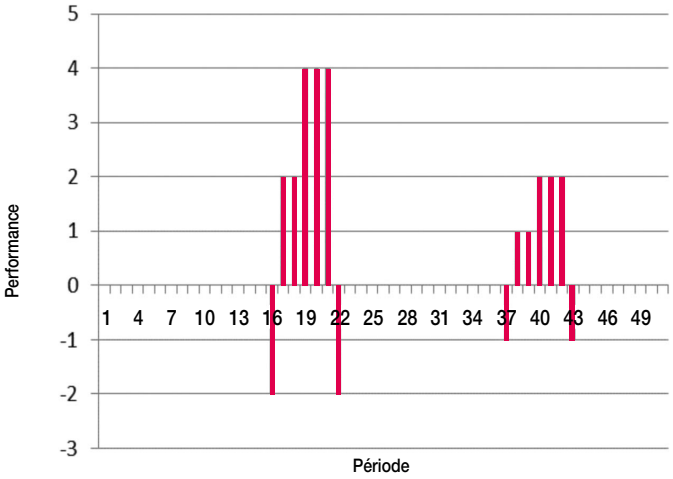
Figure 2 - Profil type d'une stratégie directionnelle : des rendements relativement symétriques et de longues périodes de gains du fait de la persistance des tendances par rapport aux périodes de rupture



Source : Scor Global Investments.

• les stratégies d'arbitrage, dans lesquelles les investisseurs vont tirer parti de la valeur relative de différents actifs, instruments, émetteurs, en se positionnant sur la convergence ou la divergence de leur valorisation vers le retour à une moyenne ou à une valeur fondamentale.

Figure 3 - Profil type d'une stratégie d'arbitrage : des rendements plus rarement positifs mais généralement plus significatifs



Source : Scor Global Investments.

Depuis plusieurs décennies, les techniques de gestion appliquées par les investisseurs ayant un passif long (sociétés d'assurance, mutuelles, fonds de pension) sont généralement basées sur des méthodes plus ou moins raffinées d'adossement du passif, avec en objectif la minimisation de l'écart de duration entre l'actif et le passif du bilan, et ont donc essentiellement reposé sur des stratégies de portage. Ceci est dû à la combinaison de plusieurs phénomènes distincts :

• d'une part, les choix stratégiques des instances managériales, dont la tendance naturelle est de privilégier la prise de risque là où se trouve le cœur du métier (côté passif), et qui se traduisent donc par une aversion prononcée pour la variabilité des résultats de l'actif, et par une moindre allocation du capital à sa composante investissement ;

• d'autre part, la réglementation de ces secteurs au travers de limitations strictes ou de charges en capital prohibitives sur les actifs les plus directionnels (actions), et pénalisant également les stratégies de retour à la moyenne en interdisant les positions de vente nue ou en limitant les investissements dans la gestion alternative ;

• enfin, l'application de schémas comptables privilégiant le portage à terme des titres de type obligataire en préservant le compte de résultat de la volatilité des prix sous-jacents, au contraire des autres stratégies, soumises, au mieux, à des règles de déclenchement automatique de reconnaissance de baisse de valeur et, au pire, à un impact direct et immédiat sur le compte de résultat.

L'univers de taux bas, voire nuls, dans lequel nombre d'acteurs sont contraints d'évoluer aujourd'hui crée de facto un nouveau paradigme dans le cadre duquel la gestion purement ALM perd de son efficacité.

En effet, dans le cas de la conjonction d'une inflation et de taux d'intérêt nominaux quasiment nuls, l'adossement de la duration du passif perd de son sens, sauf à considérer que les taux longs peuvent évoluer durablement en territoire négatif.

Ainsi, si l'on prend par exemple le cas d'un assureur qui aurait une duration de son passif de six ans, annihiler le risque de taux le conduira à investir son actif sur le taux sans risque de même duration. Si l'on considère ce taux comme étant celui de la courbe des emprunts d'État allemands, alors la rémunération tirée de ses placements sera de zéro. Des placements rémunérés à zéro ne permettent que difficilement aux acteurs d'atteindre leurs objectifs de rentabilité et pourraient même entraîner une détérioration de leur solvabilité à moyen ou long terme.

Dans ce cadre, les investisseurs institutionnels font face à un défi majeur qu'ils pourront aborder au travers de différentes actions dont les principales sont :

- l'accroissement de l'efficacité et du rendement de leurs stratégies de portage, dans le cadre d'une gestion utilisant des produits et des techniques de plus en plus complexes ;

- la négociation d'une modification des règles de solvabilité, afin de redonner des capacités d'investissement aux assureurs sur les stratégies directionnelles et d'arbitrages ;

- l'obtention de changements de règles comptables, permettant un traitement moins pénalisant de certaines classes d'actifs (actions) ou de certains types de produits (dérivés).

D'un point de vue pragmatique, à court terme, la seule action sur laquelle les investisseurs institutionnels semblent pouvoir agir de manière significative est d'accroître le rendement de leur portefeuille, à travers l'utilisation et la combinaison de nouveaux risques tels que :

- l'allongement de la duration ;

- l'accroissement du risque de crédit ;

- l'introduction du risque de liquidité ;

- l'arbitrage de bases ;

- l'introduction de classes d'actifs au remboursement de principal non prédéfini ;

- l'exposition à des risques alternatifs.

Néanmoins, l'accroissement du rendement induisant de facto une prise de risque plus importante, il nécessite un accroissement parfois significatif du capital alloué qui varie non seulement selon les stratégies utilisées mais aussi suivant les modèles à appliquer, lesquels diffèrent selon les régulateurs et les agences de rating. L'optimisation du capital alloué est donc une composante déterminante dans la gestion d'actif en univers de taux bas et peut parfois exclure toute allocation significative à certaines stratégies.

Allonger la duration de l'actif par rapport au passif

Cela permet d'investir sur les parties très longues des courbes où les taux sont encore positifs. Cette solution a l'avantage de la simplicité et permet de déployer des tailles très importantes rapidement. En revanche, le gain additionnel de rendement par unité supplémentaire de risque est désormais relativement limité et dépend de la pente de la courbe de taux.

Si nous reprenons le cas d'un assureur de la zone euro ayant une duration de six ans, créer un gap d'ALM positif (duration de l'actif supérieur au passif) lui rapportera de 10 à 15 points de base de rendement supplémentaire par année. Ainsi, en investissant sur des obligations ayant une duration de dix ans, il pourra espérer un rendement additionnel (et absolu) de 0,5 % pour un écart de duration de quatre ans. Ce qui est évidemment peu élevé, mais est également générateur de plusieurs risques aux conséquences dommageables.

Avec un portage de 50 points de base et une pente de 15 points de base par an au mieux, si l'on prend l'hypothèse, à horizon un an, d'une courbe de taux

inchangée, alors le rendement total de cet investissement est de l'ordre de 1,9 % sur la période (effet portage de 0,5 % + effet de la pente de la courbe de taux de 1,4 %). Sur le même horizon, il suffit donc d'une hausse des taux à dix ans de 20 points de base de 0,5 % à 0,7 % pour compenser entièrement ce gain (1,9 %/9,5).

Dans le cas d'une hausse de taux, même minime, ces nouveaux investissements ne génèreront pas de perte dans le compte de résultat, du fait des normes comptables protectrices pour les investissements obligataires. En revanche, toute réduction ultérieure de ce non appariement génèrera une perte comptable difficilement acceptable, qui aura pour conséquence de ne pas pouvoir modifier la position, donc de geler les décisions d'investissement, et figera jusqu'à maturité le rendement (très faible) obtenu à l'achat.

Accroître le risque de crédit

Ce risque est celui qui a été le plus utilisé ces dernières années pour accroître le rendement des portefeuilles. Contrairement aux courbes de taux, les courbes de *spread* de crédit ne sont pas à leur niveau le plus bas. En effet, si l'on se réfère à l'indice crédit IG euro calculé par la banque BOA-Merrill (ER00), l'écart de rendement contre titre d'État (Allemagne) est de 100 points de base, soit un niveau bien plus serré que le plus haut atteint fin 2008 (430 points de base), mais encore au-dessus des niveaux des années 2000-2006 (50 à 80 points de base).

Ainsi, même si des modifications significatives du marché du crédit peuvent expliquer ce niveau historique encore relativement élevé, comme la dégradation de la qualité moyenne des émetteurs ou bien encore le nouveau caractère *bail-in-able* des dettes bancaires de rang senior, il n'en reste pas moins que ces marges restent un vecteur efficace d'accroissement du rendement.

En appliquant la même méthodologie de calcul de point mort que précédemment, les niveaux de marge actuels protègent d'un écartement de *spread* de crédit de 40 points de base, soit un retour aux niveaux de fin 2012 (145 points de base au 31 décembre 2012 pour l'indice ER00).

Enfin, si l'on veut tester l'opportunité de cet investissement en mettant en perspective l'occurrence des défauts des émetteurs privés, nous pouvons considérer ces niveaux de *spread* comme la contrepartie du risque de défaut implicite.

Sur cinq ans, le portage additionnel créé par ce risque de crédit est donc de près de 5 % cumulé, alors que les statistiques historiques sur la période 1982-2010, telles que calculées par Moody's (taux de défaut et taux de recouvrement moyen calculés en fonction de la taille des émissions), font état de pertes réelles cumulées sur cinq ans de 0,6 % pour la catégorie non spéculative.

Ainsi, malgré le resserrement continu des marges de crédit depuis 2011, le rendement supplémentaire que procure ce risque semble donc bien plus intéressant que l'extension de la duration. Il est néanmoins beaucoup plus encadré par la réglementation et peut générer des charges en capital relativement élevées si des investissements sont réalisés sur la partie spéculative, voire punitives s'ils le sont via des structures procurant du levier sur ce risque par du *tranching* de portefeuille (CDO, CLO). Et ce, alors même que ces structures seraient certainement les plus à même de procurer des rendements significativement supérieurs pour le risque qu'elles portent désormais, notamment pour les tranches hautes.

Ainsi, une détérioration de la qualité de crédit d'un portefeuille de A à BBB provoque, sous Solvabilité II, une hausse de SCR identique à celle de l'extension d'une duration de dix années, pour un rendement additionnel supérieur et un risque/rendement qui semble bien plus optimal. Cette pénalisation relative du crédit par rapport aux obligations d'État pousse donc les investisseurs à choisir l'actif ayant le couple risque/rendement le moins attractif.

Introduire du risque de liquidité

Les dernières évolutions de la réglementation bancaire pénalisent plus fortement le portage par les banques de leurs positions. Celles-ci sont ainsi à la recherche de solutions et donc de contreparties à même de porter ce risque. De nombreux assureurs ou fonds de pension, grâce à leur bonne visibilité sur leur passif, peuvent donc monétiser cet avantage en entrant dans différents types de transactions les conduisant à abandonner partiellement une liquidité dont ils ont un moindre besoin que les banques.

Peu de différence est encore faite entre actif liquide et peu liquide d'un point de vue prudentiel, ce qui permet à l'investisseur institutionnel de construire des stratégies optimisant le rendement sous contrainte de capital alloué. Ainsi, le marché des créances privées permet de combiner à la fois une marge de crédit, dont nous avons vu qu'elle reste rémunératrice pour son risque de perte associé [taux de défaut * (1 – taux de recouvrement)], et une marge additionnelle due à la faible liquidité et parfois même incessibilité de la créance. Cela se trouve renforcé par le fait qu'à notation de crédit équivalente, les créances privées sont bien souvent assorties de sûretés et de conditions protectrices qui minimisent fortement leur perte potentielle, grâce à un taux de recouvrement en cas de défaut qui s'établit historiquement autour de 70 % à 80 % contre 30 % à 40 % pour les dettes obligataires classiques. Dans ce cadre, le cas des dettes privées de financement d'infrastructure est particulièrement éclairant avec des rendements supérieurs de 175 points de base par rapport à leur taux sans risque pour une notation équivalente de BBB/BBB- ; et un taux de recouvrement espéré en cas de défaut (R) de près de 80 %, à comparer avec un *spread* moyen de seulement 100 points de base pour une émission obligataire classique de même maturité et de même notation avec un R de seulement 40 %.

Arbitrer les risques de base

Ces risques permettent de capturer une marge de rendement supplémentaire en profitant des phénomènes de segmentation affectant certains marchés et ne permettant pas d'arbitrage parfait.

Dans ce domaine, l'une des techniques les plus utilisées consiste en l'achat d'émissions libellées dans une autre devise que celle de son portefeuille, et de swapper tous les flux de cash dans sa devise de référence. Suivant les inefficiences de marché, l'investisseur pourra alors, en conservant ses positions jusqu'à maturité, accroître le rendement de son portefeuille pour le même risque de crédit sous-jacent (en ajoutant néanmoins du risque de gestion du collatéral et de contrepartie).

Ainsi, si l'on prend le cas des émissions Telecom Italia aujourd'hui, l'obligation 2017 en livre britannique, une fois asset swappée en euro fixe, donne un taux de 1,96 % à maturité, alors que les émissions Telecom Italia 2017 en euro donnent un taux de seulement 1,37 %. En effet, le *spread* de cette souche est de 80 points de base plus large contre le Gilt de même maturité par rapport à la souche euro contre bund duquel on peut schématiquement déduire le taux de *basis swap* entre la livre britannique et l'euro (20b). Un tel investissement procurera donc environ 60 points de base de rendement additionnel.

La limite de cette stratégie est bien souvent comptable, car les variations de prix de la patte *swap* impacteront le résultat de l'assureur et pas l'obligation, sauf à opter pour une technique dite de *hedge accounting* ou bien à utiliser des structures ad hoc de type SPVs, mais sachant que cela comporte des risques de requalification significatifs.

Une autre stratégie, peu mise en place par les investisseurs institutionnels du fait de la nature des produits utilisés, est le portage des bases existant entre le marché des CDS et celui des obligations

sous-jacentes. Ainsi, l'achat d'une obligation Vinci 3,375 % à échéance mars 2020 permet d'avoir un rendement total de 0,62 % ; alors que son équivalent synthétique, comportant la vente d'un CDS cinq ans sur ce même émetteur (0,73 %) et le *swap* variable-fixe du cash nominal sous-jacent à cinq ans (0,28%) rapporte 1 %, soit près de 40 points de base de plus.

Ici encore, cela nécessite une gestion supplémentaire du risque de collatéral et de contrepartie auquel se rajoute la limite comptable qui implique des impacts potentiellement non négligeables sur le résultat.

Introduire des classes d'actifs au remboursement de principal non prédéfini

Dans cette catégorie se retrouvent les supports d'investissement distribuant des cash-flows plus ou moins récurrents mais n'ayant pas de maturité légale et donc pas de remboursement de principal connu à l'avance. Ces classes d'actifs comportent donc une composante portage pouvant être en revanche entièrement annihilée par la volatilité de leur composante directionnelle.

Les principales classes d'actifs regroupées dans cette catégorie sont les devises, l'immobilier et les actions avec des caractéristiques de rendement très différentes.

Le rendement des devises

En investissant sur des actifs libellés dans des devises où les taux courts sont plus élevés, l'investisseur peut bénéficier d'un portage plus important.

Outre le fait que la volatilité du taux de change impacte directement le compte de résultat, son imprédictibilité rend difficile toute allocation significative. Les investisseurs japonais ont appliqué cette stratégie dans les années 2000, mais ils bénéficiaient du fait d'être la seule zone évoluant en univers de taux bas et leur position de portage pouvait s'appuyer sur des actifs en dollar ou en euro. La baisse généralisée des taux dans les pays développés limite désormais cette stratégie à des investissements dans des actifs de pays émergents tels que le Brésil ou la Turquie, où la volatilité à attendre du taux de change est extrêmement élevée. Ainsi, la dimension « portage » de cette stratégie peut être complètement dominée par la dimension directionnelle. Un investissement dans un titre court de l'État brésilien rapporte ainsi près de 12 % par an s'il est libellé en réal, alors qu'il ne rapporte que 1,5 % s'il est libellé en dollar. En revanche, sur l'année 2014, l'évolution du réal brésilien par rapport au dollar américain a été une baisse de près de 10,6 %.

Le rendement de l'immobilier

L'immobilier bénéficie d'une forte récurrence des cash-flows, du fait notamment de la durée des baux qui, même s'ils peuvent être révisés, procurent une forte visibilité et permettent d'envisager réellement son investissement sous un angle de rendement pur. Pour un assureur, la charge en capital ou le schéma comptable sont relativement protecteurs et permettent donc des allocations significatives. En revanche, la forte appréciation des prix de l'immobilier, notamment en France, et la sensibilité négative de ses prix aux taux d'intérêt accroissent le risque directionnel de cet investissement. Ainsi, une stratégie d'allocation significative à l'immobilier doit désormais se placer dans le cadre d'une diversification géographique prononcée.

Le rendement des actions

Du fait de la volatilité des marchés actions qui peut être très élevée, une stratégie de rendement sur ce sous-jacent se trouve bien souvent confrontée à une prédominance forte de la composante directionnelle. Ainsi, même si le taux de dividende actuel des actions européennes est relativement élevé en étant même supérieur au taux de rendement de leurs

obligations de référence, cette stratégie ne peut s'envisager que sur un horizon très long terme voire infini. En effet, avec des volatilités annualisées d'indices actions de 15 % à 20 % en moyenne et des rendements de dividendes de 3 %-4 %, l'effet prix est tout à fait dominant. De plus, non seulement les charges en capital sont élevées sur les actions (autour de 40 % dans les modèles des agences de rating ou sous Solvabilité II), mais les normes comptables IFRS actuelles sont également pénalisantes. En effet, elles obligent à constater la perte de valeur dans le compte de résultat, lorsque l'action sous-jacente a provoqué une perte au-delà de seuils définis sur différentes périodes de détention relativement courtes. Cette situation pourrait même encore se détériorer avec les nouvelles normes comptables à venir IFRS9, qui édicteraient comme principe général pour les actions un impact direct et sans condition dans le compte de résultat. Et même si ces règles semblent laisser la place à un principe dérogatoire permettant sous conditions de ne jamais impacter le résultat (ni du fait de dépassement de seuils, ni du fait de la cession des titres), et donc de reconnaître les stratégies de long terme, il ne pourra que difficilement permettre la construction de stratégies actions ayant pour but d'accroître le rendement récurrent.

Une exposition à des risques alternatifs

Certains marchés, encore confidentiels, commencent à être utilisés pour leurs profils de risque de type portage et leur non corrélation avec la grande majorité des autres risques du portefeuille. Dans ce cadre, le marché des *insurance linked securities*, dont le segment le plus connu sont les obligations catastrophes, permet d'obtenir un rendement significatif, généralement entre 4 % et 8 % au-dessus du taux sans risque, en fonction de la probabilité d'occurrence des risques couverts. Tout comme pour une obligation crédit classique, la rémunération supplémentaire au taux sans risque est due à la rémunération d'un risque de perte partielle ou totale de l'investissement. La différence majeure étant que l'événement déclenchant la perte n'est plus un défaut ou une restructuration de la dette de l'émetteur, mais l'occurrence d'une ou plusieurs catastrophes naturelles sur une zone et une période précises, et le dépassement de seuils paramétriques prédéfinis ou de pertes chez un assureur donné ou sur l'ensemble des pertes assurées.

De facto non corrélées aux autres classes d'actifs, par la nature même du risque auquel l'investisseur est exposé, les obligations catastrophes sont de plus en plus présentes dans les allocations de portefeuille des fonds de pension et caisses de retraite suisses et scandinaves et peuvent représenter de 1 % à 5 % de leurs actifs.

Ainsi, dans cet environnement de taux bas qui semble pérenne, une des mutations importantes à opérer par nombre d'investisseurs institutionnels est de passer d'une stratégie classique relativement passive d'adossement à une gestion de type « rendement absolu » s'appuyant sur de multiples sources de performance et nécessitant une gestion plus active des portefeuilles, en privilégiant, du fait des contraintes existantes, une combinaison de risque de crédit, de liquidité et de risques alternatifs.

Cette complexification des positions et des outils requiert une forte compétence et une maîtrise stricte des risques, ainsi qu'une nécessité croissante d'analyser son portefeuille non seulement dans sa dimension d'allocation d'actif, mais aussi dans sa dimension factorielle et dans ses composantes individuelles.

En outre, elle nécessite une allocation de capital plus importante aux portefeuilles d'investissement, et donc un arbitrage du management entre le risque porté par l'activité d'assurance (le passif) et celui porté par l'investissement (l'actif).

Ainsi, les investisseurs institutionnels vont devoir externaliser des parties de plus en plus importantes de la gestion de leur actif auprès de gérants spécialisés et/ou développer de fortes expertises en interne. C'est ce dernier choix qui a été fait chez Scor Global Investments, où des équipes fortement spécialisées sur les *insurance linked securities*, sur les marchés du

crédit en général et sur les créances privées en particulier complètent celles présentes sur les produits de taux plus classiques, et regroupent désormais une cinquantaine de collaborateurs.

Néanmoins, malgré les efforts de l'industrie, si l'environnement de taux extrêmement bas devait se prolonger, seuls une redéfinition des règles prudentielles encadrant la gestion de l'actif et un assouplissement des règles comptables permettront aux acteurs institutionnels d'accroître significativement le rendement espéré de leur portefeuille en cessant de les pousser à investir sur les obligations d'État dont le ratio rendement/risque est l'un des plus faibles qui soit.

4.

Études et débats

Actualité de la Fondation du risque

Livres

L'ASSURANCE SANTÉ EN ESPAGNE

Jean-Pierre Daniel

Directeur commercial, Agrupació (1)

Il y a quelques années, les assureurs santé français allaient observer les HMO (2) *américains en pensant que ces gestionnaires de réseaux de soins leur transmettraient des méthodes utiles pour le futur. Ils auraient pu se rendre moins loin, puisque l'Espagne connaît depuis très longtemps un système d'assurance santé privé qui se substitue à la Sécurité sociale. Ainsi, on peut apprendre beaucoup des pratiques du marché espagnol, qui développe ses produits dans un contexte concurrentiel où les hommes de marketing écoutent, s'ils ne les devancent pas, les besoins du client. Cependant, on perçoit aujourd'hui les limites du système, et certains assureurs commencent à expérimenter des solutions de complémentarité entre secteur public et secteur privé, au niveau des produits mais aussi au niveau de la gestion de l'offre de soins.*

Le système actuel

L'Espagne connaît un système de sécurité sociale universelle dont bénéficie toute personne résidant sur le territoire. Le financement est assuré par l'impôt et non par des cotisations assises sur les revenus du travail. Les soins sont gratuits dans tous les cas, à l'exception du dentaire, qui n'est pas pris en charge. Certains médicaments sont remboursés par la Sécurité sociale, d'autres non, et il existe des mécanismes de prise en charge plus généreuse pour certaines catégories sociales plus fragiles, comme les retraités. La contrepartie de cette gratuité est que la Sécurité sociale affecte à chaque bénéficiaire un médecin généraliste et que celui-ci fait office de *gatekeeper* (3) pour accéder aux examens, aux hôpitaux et aux spécialistes. C'est un parfait exemple de médecine de caisse qui engendre les files d'attente caractéristiques de toutes les médecines de caisse. Le malade en urgence ou en traitement contre le cancer est parfaitement bien pris en charge, l'Espagne ayant hérité de ses envahisseurs arabes une médecine de pointe de très grande qualité. Si en revanche un individu contracte la grippe dans une grande ville, la maladie se sera soignée toute seule avant qu'il ait pu obtenir un rendez-vous chez son médecin référent.

C'est pour répondre à ce besoin de rapidité et de commodité, et aussi de confort dans le cadre des hospitalisations, que se sont développées les assurances santé privées. Depuis la fin du XIXe siècle existaient des *igualatorios* créés par des médecins qui, sur la base de la capitation, soignaient « gratuitement » les habitants d'un village ou les salariés d'une entreprise, comme les premiers HMO américains. Soit le patron payait pour ses ouvriers, soit chaque habitant du village payait son obole au médecin local. Certains de ces *igualatorios* existent encore aujourd'hui de manière

plus ou moins artisanale, puisque les corps de contrôle de l'assurance considèrent que la capitation ne doit pas être utilisée comme mode de financement de l'assurance maladie.

Les deux principaux produits

Sur ce marché, où les sociétés de santé actuelles ne ressemblent en rien aux *igualatorios*, deux types de garantie sont proposés, l'*asistencia sanitaria*, qui est de très loin la formule dominante, et une formule dite de *reembolso*, qui est une assurance au premier euro. On s'étendra plus longuement sur l'*asistencia sanitaria* car c'est elle qui présente le plus d'originalité. L'assureur met à la disposition de l'assuré un réseau de médecins, laboratoires, hôpitaux, kinésithérapeutes et, dans certains cas, dentistes. Ces réseaux regroupent de très nombreux praticiens et couvrent en principe tout le territoire, afin que le client en déplacement trouve un médecin près de son lieu de résidence. Les sociétés ont entre 20 000 et 35 000 médecins référencés, et la dimension du réseau est un argument commercial majeur. La mère veut y trouver le pédiatre en qui elle a confiance et la femme le gynécologue qu'elle consulte régulièrement. Dans la mesure où le pays compte 173 000 médecins, il est normal qu'un même praticien collabore avec plusieurs sociétés. Il consulte même souvent à la Sécurité sociale le matin et en libéral l'après-midi.

Si le client s'adresse à l'un des médecins du réseau, en principe, il ne paie pas la visite. Il ne débourse rien. Grâce à une carte magnétique, le médecin est payé directement par l'assureur. Il existe des formules de contrats comportant une franchise, ce que nous appellerions un ticket modérateur. Elles sont évidemment moins chères, puisque le coût de la visite est moindre pour l'assureur et surtout parce que l'existence même de la franchise réduit la consommation médicale. Dans certains de ces contrats, le montant annuel des franchises est limité, de sorte qu'en cas de vrai problème de santé le client est totalement pris en charge. En dépit du fait qu'ils obéissent clairement à une logique économique, les produits avec franchise peinent à se développer. L'explication que l'on donne est que si un client a la capacité économique de payer un contrat santé, il veut être couvert pour tout et sans rien débourser. Ce principe de gratuité au moment de l'utilisation du service qui vaut chez le médecin vaut aussi, bien sûr, pour les examens ou les hospitalisations dans les établissements du réseau de la société d'assurance.

Au niveau des garanties offertes, le marché est totalement libre. La seule exigence est que le contrat doit couvrir sans délai de carence les urgences vitales. Selon les politiques des entreprises et le prix du produit, les garanties sont plus ou moins complètes, mais la différenciation se fait surtout par des prestations un peu marginales, car tous les contrats proposent d'emblée un très bon socle de garanties. On peut offrir des séances de psychologue, de podologue, des visites d'homéopathie ou la prise en charge de la reproduction assistée. Il y a logiquement des phénomènes de mode, comme aujourd'hui la conservation des cellules souches du cordon ombilical.

Sur le plan technique, la gestion de cette forme d'assurance est bien différente de celle d'une assurance de personnes traditionnelle. Le premier point est qu'il s'agit de la santé de l'assuré et de sa famille, ce qui explique une très grande sensibilité du client au moment de la gestion du sinistre. Quand une mère appelle parce que son enfant est malade, c'est la plateforme médicale de l'assureur qui décide s'il faut envoyer une ambulance et aller vers les urgences, ou si cela peut attendre la visite du généraliste le lendemain matin. Une autre des difficultés est que la prestation n'est pas faite par l'assureur mais par un prestataire. Il faut pouvoir contrôler la qualité du service, mais il faut aussi contrôler le prestataire. Si le client paie une prime fixe, le médecin ou le laboratoire sont payés à l'acte. Ni en France ni en Espagne les médecins ne sont de purs esprits, et l'assureur se doit de vérifier que la consommation générée par tel praticien ne s'écarte pas trop de celle de ses confrères situés dans la même région. Un point enfin où la différence avec l'assurance traditionnelle est patente c'est que le coût des sinistres dépend de la taille de l'entreprise. Une société très puissante, capable de

promettre à un médecin l'envoi de nombreux clients, obtiendra de ce médecin de meilleures conditions qu'un opérateur plus modeste. Les sociétés ne communiquent pas sur ce qu'elles paient à leurs médecins, mais sur le marché on estime que, pour une visite de généraliste, l'écart peut représenter de 5 à 20 euros selon la taille de l'entreprise.

L'autre système de prise en charge des soins est plus simple. Il s'agit de ce que l'on appelle *reembolso*, qui est une assurance au premier euro. Dans la quasi-totalité des cas, il y a un reste à charge de 10 % à 20 % du prix de la visite payé par le patient, qui est libre de voir le médecin de son choix. Cependant, ce reste à charge est supprimé si le patient consulte un prestataire qui appartient au réseau médical de l'assureur. Vu la taille de ces réseaux, il est très fréquent que le client de ce type de contrat consulte au sein du réseau. Certes, il ne supporte pas la franchise, mais l'assureur paie le médecin au prix convenu pour l'ensemble de ses prestations. Comme ces contrats au premier euro sont vendus sensiblement plus chers que les contrats classiques et que, de fait, l'assuré les utilise comme un contrat classique, cette modalité donne de meilleurs résultats techniques.

Quelques chiffres

Le chiffre d'affaires total de l'assurance santé en Espagne en 2014 est de 7,175 milliards d'euros, soit 23,5 % du chiffre d'affaires IARD :
- 78,5 % correspondent à l'*asistencia sanitaria*
- 6,7 % au *reembolso*
- 14,7 % aux indemnités journalières*

Nombre d'assurés : 10,4 millions, soit 22 % de la population.
27 % du coût de la santé est pris en charge par le secteur privé.

Rapport sinistres à primes :
- 80,7 % en *asistencia sanitaria*
- 69,8 % en *reembolso*

Le marché est très concentré : les 5 premiers acteurs totalisent 71,4 % du marché.

** L'assurance des indemnités journalières ne présente aucune spécificité sur le marché espagnol, et on ne l'a pas prise en compte dans cet article.*

Les difficultés qui expliquent une évolution

Comme le montrent les chiffres cités dans l'encadré, les résultats techniques en *asistencia sanitaria*, où se concentre l'essentiel du portefeuille, ne sont pas vraiment bons alors que les primes, élevées en valeur absolue, ne peuvent guère être augmentées. Il existe bien entendu une totale liberté tarifaire, et, comme les contrats sont plus ou moins complets, on trouve tous les tarifs sur le marché. Pour donner un ordre de grandeur au lecteur français, pour un contrat complet « classique », la prime mensuelle pour une personne de 40 ans se situera entre 40 et 50 euros. À l'année, cela suppose entre 500 et 600 euros pour chaque membre de la famille, ce qui représente un total compris entre 1 500 et 2 000 euros par an, selon le nombre d'enfants. Les tarifs sont désormais unisexes bien que les femmes consomment plus, et ils varient bien entendu avec l'âge, jusqu'à devenir économiquement insupportables pour une personne âgée. De fait, si on compare ces tarifs avec ceux des complémentaires santé françaises, on constate que les prix en Espagne sont en vérité tout à fait modérés, puisque l'assureur se substitue totalement à la Sécurité sociale. Le client de l'assureur privé ne coûte rien à la Sécurité sociale. La seule exception étant les traitements très lourds, pour lesquels les Espagnols préfèrent la médecine de pointe des grands hôpitaux publics, même si le confort de la chambre est moindre que dans une clinique privée.

Chaque année ces tarifs augmentent de quelques points pour tenir compte de l'évolution des techniques médicales. La santé est même la seule branche à croître dans l'assurance espagnole, durement frappée par la crise économique, ce qui pousse les

clients à réduire leurs garanties. Le niveau élevé de cette prime en valeur absolue, dans un pays où chaque citoyen peut accéder gratuitement à la Sécurité sociale, constitue le principal défi pour ceux des assureurs santé qui se projettent dans l'avenir. Ils craignent que les citoyens finissent par refuser de payer deux fois – par l'impôt d'abord et par l'assurance privée ensuite – le coût de leur santé.

Sur le plan commercial, on observe depuis des années une quasi-stagnation du nombre des assurés, alors que les assureurs se livrent à une bataille farouche pour conquérir des clients. En fait, les clients se déplacent d'un assureur à l'autre, sans croissance du marché global. Tout se passe comme si ceux qui ont déjà un contrat santé voulaient le garder, si possible en payant moins cher chez un assureur concurrent, alors que les sociétés ne parviennent pas à assurer des gens qui ne le sont pas.

Les premiers pas vers une complémentarité

Ce constat a conduit plusieurs sociétés à offrir des produits qui ne se substituent pas totalement à la Sécurité sociale et qui, de ce fait, sont beaucoup moins chers. On voit ainsi apparaître des contrats qui ne couvrent que la médecine ambulatoire. Ils visent une clientèle habitant les grandes villes, où l'accès au médecin de la Sécurité sociale est très long. Pour tous les problèmes de santé courants, le client est pris en change rapidement. S'il doit être hospitalisé, il faut recourir à la Sécurité sociale. D'autres produits se positionnent exactement à l'envers. Ils visent les habitants des petites villes, où souvent le médecin de la Sécurité sociale est plus accessible mais où l'hôpital local laisse à désirer. Le contrat ne couvre que l'hospitalisation en laissant bien entendu au malade le choix de son établissement. Pour l'instant, la part de marché de ces nouveaux produits reste marginale par rapport au portefeuille constitué de contrats traditionnels, mais beaucoup d'assureurs y voient une solution d'avenir. Il en va de même des contrats avec franchise, dont on a dit qu'ils peinent à se développer mais dont on peut être sûr qu'ils connaîtront une croissance significative dans les années qui viennent.

Si l'on quitte maintenant le niveau des produits pour se situer au niveau des prestataires, on constate des rapprochements entre le secteur public et le secteur privé qui correspondent aussi à une recherche de complémentarité.

L'exemple le plus ancien est celui de l'assurance des fonctionnaires. Ceux-ci bénéficient d'un régime particulier de sécurité sociale géré par une mutuelle – Muface – qui reçoit son budget de l'État. Chaque année, Muface organise un appel d'offres pour proposer aux assureurs privés d'offrir les mêmes services que la Sécurité sociale à un prix fixé par Muface. Aujourd'hui, quatre sociétés participent à ce régime qui concerne plus d'un million et demi de fonctionnaires et leurs familles. Chaque fonctionnaire a le choix entre rester dans le cadre de la Sécurité sociale ou recourir à l'un de ces assureurs privés. Plus de 80 % font le choix du privé, ce qui dit bien la mauvaise image du secteur public. Ce mécanisme est comparable à une concession de service public, l'entité privée s'engageant à fournir une prestation selon un cahier des charges et un prix fixé par l'Administration.

Plus récente et plus originale est l'entrée des opérateurs privés dans la gestion des hôpitaux publics. La plupart des sociétés d'assurance santé possèdent des hôpitaux, des cliniques et des centres de soins. C'est un moyen de se donner de la visibilité sur le plan commercial, d'apporter un service à leurs assurés et de contrôler les coûts, puisque dans ces établissements le personnel est salarié de l'assureur. Ce n'est pas novateur et cela évoque les cliniques mutualistes qui existent en France. Ce qu'il est plus intéressant d'observer c'est que, dans certaines régions, on voit des assureurs privés s'intéresser à la gestion de la totalité de la santé de la population.

La santé fait partie des compétences dévolues aux régions autonomes, et le Levant, dont la capitale est

Valence, est en pointe dans ce domaine. Depuis 1999, Adeslas, la première entité du marché, est gestionnaire d'un hôpital créé par le gouvernement régional. La société est rémunérée par un système de capitation, et les patients sont traités gratuitement, comme ils le seraient dans un hôpital géré par la Sécurité sociale. Dans une partie de cette même région, Sanitas, filiale de Bupa et deuxième acteur du marché, gère un hôpital généraliste, 22 cabinets médicaux et un hôpital de long séjour pour une population de près de 200 000 habitants. Dans la même région, Asisa, coopérative de médecins et troisième société du marché, gère la santé des 160 000 habitants de la zone de Torrevieja avec un hôpital et dix cabinets médicaux. La même entreprise gère pour le compte de la Sécurité sociale deux hôpitaux en se contentant d'un rôle de gestionnaire, l'investissement initial étant réalisé par l'Administration. La société allemande DKV, autre grand acteur du marché, gère aussi un hôpital. À une échelle plus modeste, il existe en Catalogne quelques expériences de cabinets médicaux où des médecins associés soignent une collectivité d'assurés pour le compte de la Sécurité sociale en contrepartie d'une rémunération forfaitaire. Toutes les enquêtes montrent la très grande satisfaction des assurés, qui sont ravis du service rendu.

Si ces expériences fonctionnent à la satisfaction des clients, il a fallu procéder à des ajustements de la relation entre la puissance publique et les sociétés d'assurance. Au cours des dernières années, la rémunération des sociétés d'assurance gestionnaires a été revue à la hausse, car celles-ci ne parvenaient pas à équilibrer leurs résultats. Il faut aussi – et surtout – tenir compte de la dimension politique. En Espagne comme en France, la santé est sacrée et elle est supposée ne pas avoir de prix. Ce n'est pas un hasard si ces expériences de concession de la gestion sanitaire au secteur privé ont eu lieu au Levant, une région gouvernée par la droite. Dans la province de Madrid, également gouvernée par la droite, existe un hôpital géré selon le régime du partenariat public-privé, mais la tentative de privatisation de six hôpitaux publics en 2013 a soulevé un tel mouvement de protestation que le gouvernement régional a dû faire machine arrière. Aujourd'hui ces projets de coopération entre public et privé, en dépit de la réussite qu'ils représentent dans la région de Valence, sont paralysés. Les gouvernements locaux considèrent que le coût politique de toute tentative de privatisation de la santé est trop élevé, et les professionnels pensent que seul un accord droite-gauche dans l'esprit du pacte de Tolède (4) permettrait à ces mécanismes de prospérer.

Ainsi, l'Espagne n'est pas un champ de roses pour les assureurs santé, qui doivent faire évoluer un modèle parfaitement rodé mais en panne de croissance. L'avenir n'est pas à une lutte ouverte entre une Sécurité sociale qui dispenserait une médecine du pauvre et une assurance privée qui offrirait chaque année des garanties nouvelles et toujours plus coûteuses. À l'évidence, l'expansion d'une assurance privée devenue complémentaire et la contention du coût global de la santé d'une population vieillissante se feront par une collaboration du public et du privé. L'État veillera à garantir un service de base et laissera au secteur privé la liberté de compléter ou d'améliorer les prestations offertes par la Sécurité sociale.

Notes

1. Société d'assurance de personnes spécialisée en assurance santé. Il s'agit d'une mutuelle installée à Barcelone qui, après avoir connu des difficultés, a été démutualisée et achetée en 2012 par le pôle des assurances du Crédit Mutuel.

2. HMO : Health Maintenance Organizations.

3. Portier.

4. Signé en 1995, le pacte de Tolède est un accord par lequel l'ensemble des forces politiques et syndicales espagnoles dessinèrent ce que devait être l'évolution du système de retraite au cours des années suivantes.

Haddock, le risque aggravé

Pierre Martin

Agrégé d'histoire, docteur en histoire

« Oui, je vous ai f-f-fait appeler, lieutenant, c'est... c'est hon-honteux ! On me... c'est honteux !... On me laisse mourir de soif !... Je... je n'ai p-p-plus une goutte de whisky...! (1) » C'est sous ce jour peu glorieux, au fond du cargo Karaboudjan, *que le capitaine Haddock apparaît pour la première fois, tristement dépendant du whisky... Haddock serait donc un risque aggravé, celui qui « [augmente] la probabilité ou l'intensité du risque (2) »... Une navigation sans sextant dans le corpus de Tintin dévoile un rapport au risque pourtant plus paradoxal qu'escompté.*

« L'alcool, ennemi du marin (3) »... et de l'assureur

De prime (!) abord, un assureur considérerait que le capitaine de la marine marchande Haddock incarne le mauvais risque par définition. Dès son apparition, dans *Le crabe aux pinces d'or*, tout dans son comportement confirme une addiction sévère à l'alcool qui lui fait perdre le sens commun. Il surexpose son entourage à la probabilité d'un sinistre. Il est bien le risque aggravé. Qu'on en juge. Il est incapable de commander le *Karaboudjan*, dirigé en réalité par le méchant lieutenant Allan Thompson… Le félon abreuve Haddock de whisky « car ainsi [il] reste le seul maître à bord (4) », libre d'organiser un trafic d'opium... Activité illicite, inassurable, mais qui aggrave le risque... Évadé avec Tintin dans un canot de sauvetage, Haddock boit la réserve de rhum et met le feu au bateau, provoquant un naufrage. Haddock récidive dans un hydravion arraisonné par Tintin : il engloutit une bouteille de whisky, qu'il fracasse (vide) sur la tête de son compagnon... Bilan : un atterrissage forcé et un avion en flammes en plein Sahara... L'attaque des guerriers bérabers confirme qu'Haddock a une conduite à risques, y compris à dos de chameau… En deux coups de feu, les pillards détruisent (5) les (dernières ?) bouteilles qu'Haddock avait manifestement subtilisées au lieutenant Delcourt, lors de leur escale salvatrice au poste méhariste d'Afghar. Cet incident mineur fait exploser le capitaine (« VENGEANCE ! »), qui se rue sur les Touaregs, sous un feu nourri, au mépris du danger. Un comportement riscophile qui surexpose Haddock à la menace ultime : « Vous allez vous faire tuer (6) », prévient Tintin. Épisode qui révèle également un caractère sanguin lui aussi facteur de risque : le capitaine lance une salve initiale de vingt jurons, soit 10 % de la collection reconstruite (7), dont le célèbre « marin d'eau douce », archétype méprisé du riscophobe (8). Selon un des meilleurs exégètes d'Hergé,

cette traversée du Sahara constituerait une étape essentielle dans le sevrage du capitaine Haddock, confronté brutalement au risque d'une mort par déshydratation. Un supplice : Haddock répète, hébété, qu'il est « au pays de la soif [9] ». Un risque d'alcoolémie qui serait finalement minimisé une fois ce désert vaincu : « Son attrait pour la boisson n'est plus qu'un aimable penchant. [10] » Voire... Dès son escale à Bagghar, au Maroc, Haddock sirote au moins une demi-bouteille dans un estaminet des quais, suffisamment pour le rendre ivre et ameuter (par deux fois) la « Po-p-p-police [11] ». Curieusement, l'alcool change de statut en ce qu'il accélère le dénouement tel un *deus ex machina*. Tintin et Haddock se retrouvent ainsi coincés dans une cave par Allan Thompson et ses complices, dont les balles percent des tonneaux. Sans boire une goutte (!), les héros se retrouvent ivres… des vapeurs d'alcool. Le vin, au lieu d'augmenter le risque en abattant Haddock, décuple ses forces. Le capitaine rosse Allan et, lancé à sa poursuite, trouve l'issue des caves... dans la maison du caïd Omar Ben Salaad. In fine, le capitaine se lance dans une conférence radiophonique sur un thème rédempteur : « L'alcool, ennemi du marin ». L'incipit recense précisément les risques de la navigation hauturière pour placer l'alcool à son sommet : « Car le pire ennemi du marin, ce n'est pas la tempête qui fait rage ; ce n'est pas la vague écumante… qui s'abat sur le pont, emportant tout sur son passage ; ce n'est pas le récif perfide caché à fleur d'eau et qui déchire le flanc du navire ; le pire ennemi du marin, c'est l'alcool ! [12] » Malheureusement, les actes ne coïncident pas avec le discours, puisque le capitaine fait un malaise en avalant un verre... d'eau. On ne connaîtra donc jamais la suite de l'argumentation qui participait apparemment de la prévention des risques chère à l'assureur. Une posture que revendique désormais Haddock, promu président de la Ligue des marins antialcooliques [13]... Les rechutes (trop) fréquentes, pour ne pas dire systématiques, montrent hélas qu'Haddock conserve son addiction alcoolique, qui l'amène à déclencher, dans le pire des cas, un sinistre. Sur le navire *Aurore*, il conserve une armoire de bouteilles de whisky [14]. Lors de son escale à Reykjavik, il réclame « une larme, un soupçon » de whisky dans son eau minérale : le verre déborde [15]. Avant d'appareiller pour découvrir le trésor de Rackham le Rouge, son médecin lui envoie diagnostic et prescriptions : « Insuffisance fonctionnelle du foie. […] Aliments défendus. Toutes boissons alcoolisées. [16] » Dans *Coke en stock*, le seul bruit d'une bouteille débouchée le fait se réveiller et engloutir une flasque de whisky – qu'il conserve sur lui régulièrement, semble-t-il [17] . On citera enfin les déboires (!) de la consommation de whisky dans la fusée partie pour la lune. Haddock, au prétexte de « travailler sérieusement », s'isole dans sa cabine pour lire un traité d'astronomie... qui cache deux bouteilles de breuvage écossais. Après une dégustation sérieuse, le whisky se met à flotter en l'air, puisque Dupont a désactivé la pesanteur artificielle. Ivre, Haddock enfile sa tenue d'astronaute, sort du vaisseau et se retrouve dans l'espace [18] : « Je r-r-retourne à Moulinsart, moi ! [19] » Résumons-nous : à terre, sur mer, dans les airs et dans l'espace, Haddock est le risque aggravé par essence qu'aucun assureur ne voudrait pour client... Une lecture plus approfondie de l'œuvre d'Hergé, richissime et complexe, révèle un Haddock moins mauvais risque qu'envisagé...

Haddock, un « homme rationnel devant le risque [20] » ?

Dès 1953, Maurice Allais, économiste français, fait progresser la théorie en creusant la notion d'aversion au risque. Contrairement aux postulats alors dominants de ses collègues américains, Allais a démontré que les choix des agents entre la probabilité faible de grands gains (mais aussi de grandes pertes) et celle de loteries aux valeurs plus centrales n'étaient pas ceux qu'une approche rationnelle laissait envisager. Ce travail a débouché sur la notion d'« aversion à l'ambiguïté », conceptualisée par Daniel Ellsberg en 1961 [Ellsberg, 1961]. Elle ouvre un champ de réflexion considérable bien plus qu'elle ne clôt le débat. Comment les individus réagissent-ils face au risque, dont il faut rappeler qu'il est probabilisable à

la différence de l'incertain [Knight, 1921] ? Comment les individus décident-ils en situation d'incertitude ? C'est là qu'Haddock ne laisse pas de surprendre. En tant que capitaine au long cours, Haddock débarrassé du fardeau alcoolique se révèle un (très) bon marin. Or, quoi de plus antinomique que l'art de piloter un navire et la prise de risque ? Tout commandant de bord sait qu'il doit avant tout « arriver à bon port ». Haddock tient lui-même le gouvernail de l'*Aurore* en pleine tempête, qu'il qualifie de « jolie brise » : « Évidemment, il faut être prudent... » Consigne réitérée auprès de l'homme de barre sommé de faire « attention aux icebergs (21) ». Cette vigilance et cette expérience lui font également éviter la collision avec le *SS Kentucky Star* (22). Vigilance, expérience : deux critères minorant le risque bien connus des assureurs… Haddock sait aussi parfaitement calculer sa route à partir d'une carte marine (23) tout en attribuant un secteur de recherches aériennes à Tintin avec la recommandation suivante : « Surtout pas d'imprudences : ne dépassez pas les limites fixées. (24) » Haddock est également réquisitionné par le ministère de la Marine lors d'une fugace apparition dans *Tintin au pays de l'or noir* : « "Ordre au capitaine Haddock de prendre le commandement du cargo untel (le nom doit rester secret) où il recevra de nouvelles instructions"... Voilà. En deux mots, je suis mobilisé. » Imagine-t-on les autorités maritimes confier un bâtiment à un ivrogne ? Marin avisé, Haddock se révèle un conducteur automobile étrangement calme au volant. En réalité, il ne conduit guère que dans *Les sept boules de cristal* : un superbe cabriolet Lincoln-Zephyr 1938 de couleur jaune, à la capote capricieuse. Il roule en ville sans s'énerver malgré une mauvaise soirée au music-hall. Il conduit surtout sans discontinuer de Moulinsart à Saint-Nazaire. Or le trajet, pluvieux, manifestement long, se déroule pour partie de nuit (25). Et Haddock résiste à l'excès de vitesse malgré la suggestion de Tintin valant encouragement : « Allons, en route, capitaine, ou nous n'arriverons jamais... » Le syndrome de « *road rage* », décrit par des psychologues américains pour désigner des comportements de conducteurs qui deviennent « fous de rage au volant », concerne uniquement le piéton Haddock. Haddock qui se fait tremper par un camionneur « nyctalope (26) ». Haddock furieux de recevoir une « cigarette allumée » jetée d'une voiture (27). Haddock renversé par Arturo Benedetto Giovanni Giuseppe Pietro Archangelo Alfredo Cartoffolli dé Milano (28). De même, Haddock, au regard des études de médecins nutritionnistes, n'a sans doute pas tort de se débarrasser du « Sani-Cola » de Laszlo Carreidas dans une plante verte. Le soda agit comme un défoliant instantané (29) . Enfin, le dernier opus de Tintin révèle un Haddock totalement déshabitué du whisky – « eau de javel », « imbuvable », « véritable poison » –, dont il dissuade la consommation à ses hôtes, qui s'en régalent, y compris Nestor, dont on comprend qu'il a l'habitude de goûter les réserves de son patron : « Il est délicieux, ce "Loch Lomond", comme d'habitude. (30) » « Qu'on ne me parle plus de whisky ! (31) » finit par lâcher Haddock, définitivement écœuré... sans se l'expliquer vraiment. « Comment se fait-il que je ne supporte plus une goutte d'alcool ? (32) » Dans un surprenant hapax, Hergé nous dévoile enfin le prénom du capitaine Haddock : « Archibald (33) »...

Haddock : bon ou mauvais risque ? Un détour par l'œuvre touffue d'Hergé nous montre un personnage complexe, plus réfléchi qu'irréfléchi, plus prudent qu'inconscient, plus intuitif qu'éruptif, davantage enclin à la précaution qu'à l'impulsion. « Il y a chez Haddock – surtout après son installation à Moulinsart – une vocation de gentleman-farmer perpétuellement contrariée. Un whisky et une bonne pipe au coin du feu, après une promenade au grand air, semblent représenter son idéal de vie le plus profond. (34) » Risque maritime endossé sans souci par le Lloyd's, risque automobile couvert au kilomètre, car Haddock est un petit rouleur : Haddock est sans conteste un bon risque de ce point de vue. Une complémentaire santé relèverait davantage du risque aggravé… Quant à une multirisque habitation, le capitaine pourrait en souscrire une à moindres frais pour son modeste appartement, entrevu dans *Le secret de la Licorne*. Mais il n'avait manifestement pas prévu de protéger le superbe château de Moulinsart, frappé par la foudre dans *L'affaire Tournesol*, sinon il aurait immédiatement évincé Séraphin Lampion, agent des assurances Mondass…

En remerciant Gaël Gratet, professeur de lettres en CPGE, pour sa relecture attentive.

Notes

1. Le crabe aux pinces d'or, *p. 22.*

2. Cf. *Charre-Serveau et Landel [2000], article « Aggravation du risque ».*

3. Le crabe aux pinces d'or, *p. 69.*

4. Op. cit., *p. 22.*

5. Op. cit., *pp. 43 et 45.*

6. Op. cit., *p. 45.*

7. Pol Vandromme en recense 169 [Vandromme, 1959]. Albert Algoud en dénombre près de 200 [Algoud, 1991].

8. « Un individu riscophobe […] [préfère] toujours la certitude à l'aléa. » Cf. *Chiappori [1997], p. 29.*

9. Six occurrences à la seule page 36 de l'album Le crabe aux pinces d'or.

10. Cf. *Peeters [2004], p. 71.*

11. Le crabe aux pinces d'or, *p. 51.*

12. Op. cit., *pp. 70 et dernière.*

13. L'étoile mystérieuse, *p. 14.*

14. Op. cit., *p. 15.*

15. Op. cit., *p. 30.*

16. Le trésor de Rackham le Rouge, *p. 11.*

17. Les sept boules de cristal : *épisode paru initialement dans* Le Soir *et non repris dans l'album.* Cf. *Peeters [2004], p. 82.*

18. « Décision téméraire de l'un des astronautes de quitter la fusée, au risque, comme Haddock, de rester définitivement en orbite. » Cf. *Farr [2011], p. 136.*

19. On a marché sur la lune, *p. 84.*

20. Cf. *Allais [1953], pp. 503-546.*

21. L'étoile mystérieuse, *p. 37.*

22. Op. cit., *pp. 25-26.*

23. De même dans Le trésor de Rackham le Rouge, *p. 27. Épisode où Haddock démontre sa capacité à utiliser un sextant, p. 29.*

24. L'étoile mystérieuse, *p. 33.*

25. « Demain matin, nous arriverons très tôt à Saint-Nazaire. » Les sept boules de cristal, *p. 63.*

26. « Nyctalope : personne ayant la faculté de voir dans la pénombre ou pendant la nuit » (Trésor de la langue française). *Employé comme juron par Haddock dans* Les sept boules de cristal, *p. 63.*

27. L'affaire Tournesol, *p. 34.*

28. Op. cit., *p. 44.*

29. Vol 714 pour Sydney, *p. 7.*

30. Tintin et les Picaros, *pp. 2 et 7.*

31. Op. cit., *p. 8.*

32. Op. cit., *p. 23.*

33. Op. cit., *p. 31.*

34. Cf. *Peeters [2004], p. 71.*

Bibliographie

ALGOUD A., *Le Haddock illustré. L'intégrale des jurons du capitaine*, Casterman, 1991.

ALLAIS M., « Le comportement de l'homme rationnel devant le risque : critique des postulats et axiomes de l'école américaine », *Econometrica*, vol. 21 (4), octobre 1953.

CHARRE-SERVEAU M. ; LANDEL J., *Lexique des termes d'assurance*, L'Argus, 2000.

CHIAPPORI P.-A., *Risque et assurance*, Flammarion, 1997.

ELLSBERG D., "Risk, Ambiguity and the Savage Axioms", *Quarterly Journal of Economics*, vol. 75 (4), novembre 1961, pp. 643-699.

FARR M., *Tintin. Le rêve et la réalité*, Éditions Moulinsart, 2011.

KNIGHT F. H., *Risk, Uncertainty, and Profit*, Houghton Mifflin, 1921.

PEETERS B., *Le monde d'Hergé*, Casterman, 2004.

VANDROMME P., *Le monde de Tintin*, Gallimard, 1959.

Big data
CORRÉLATION OU CAUSALITÉ

Arthur Charpentier

Professeur d'actuariat à l'Université du Québec, Montréal

Amadou Diogo Barry

Chercheur à l'Institut de santé publique du Québec

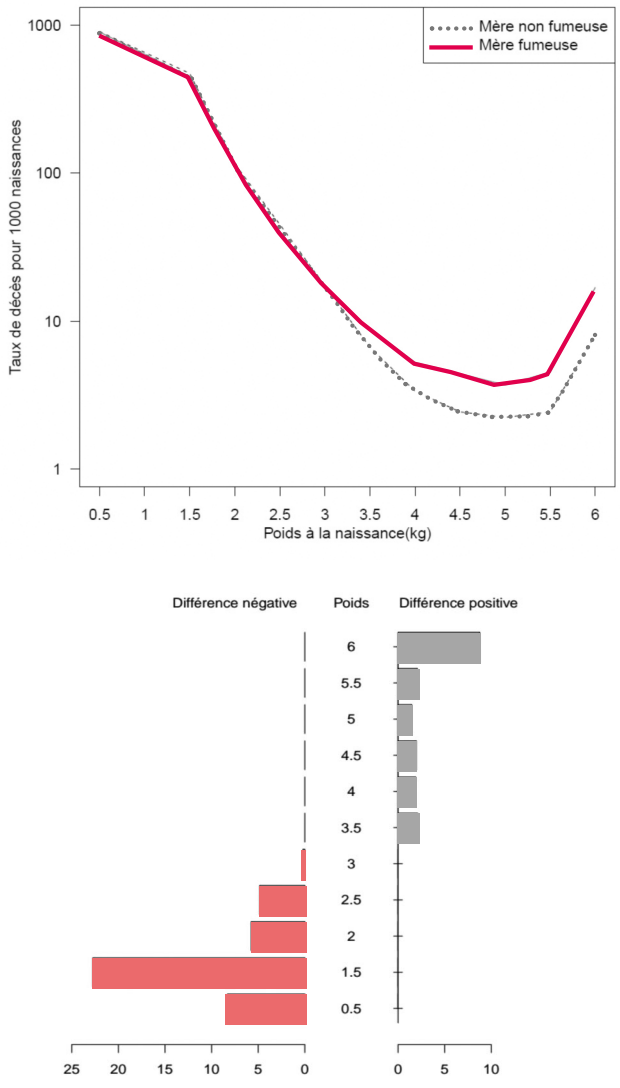
Le rôle d'un actuaire dans une entreprise d'assurance est assez souvent d'estimer la probabilité qu'un événement survienne, ou ses possibles conséquences financières, et est également fonction de variables dites « explicatives ». On voit en effet que certaines variables sont « statistiquement corrélées » avec la survenance d'un accident dans l'année, mais prétendre que l'on dispose d'une « explication » est un peu dangereux. Ce sont pourtant les interrogations qui étaient soulevées lors des débats sur la prise en compte du sexe des assurés dans la tarification automobile : si les femmes ont moins d'accidents, en moyenne, que les hommes, pourquoi ne pas utiliser cette variable en tarification ? Le problème est que s'arrêter à une étude des corrélations ne permet pas de comprendre ce qui se cache vraiment derrière un phénomène. Charpentier [2014] notait que de telles études pouvaient conduire à des interprétations paradoxales et erronées.

Ainsi que le notait Dubuisson [2008], « comme le reconnaissent les actuaires, la mise en évidence d'un lien causal entre le critère choisi et la variation de la sinistralité s'apparente à la quête du Graal ». Les données massives, le big data, *permettent peut-être d'avoir accès à davantage d'information et de mieux comprendre ce qui peut causer un risque. Un exemple classique est un paradoxe, qui a longtemps laissé les épidémiologistes perplexes, sur la mortalité infantile, le poids des bébés et le tabagisme de la mère. Nous allons reprendre cet exemple ici et analyser comment l'utilisation de données massives a permis de mieux comprendre ce qui pouvait réellement causer une surmortalité infantile.*

Le paradoxe du tabagisme et du poids à la naissance

Le poids des bébés à la naissance est considéré comme un prédicteur important concernant la survie de l'enfant. Une autre information importante est liée au tabagisme maternel. Si l'on regarde le taux de mortalité infantile, selon le poids à la naissance, en fonction du tabagisme de la mère, on obtient le graphique de la figure 1.

Figure 1 - taux de décès (échelle logarithmique) en fonction du poids à la naissance en haut, et différence entre les taux selon que la mère est fumeuse ou pas (en bas)



Source : auteurs.

Cette figure a été obtenue à partir des données mises en libre accès sur le site du CDC (Centers for Disease Control and Prevention), contenant des informations sur toutes les naissances sur le sol américain, soit près de 4 millions d'observations par an, et plusieurs centaines de variables (dont le poids à la naissance et des informations socio-économiques sur la mère). L'analyse chiffrée porte ici sur les données de 1989.

Si on exclut les « gros bébés » (de plus de 5 kg), le taux de décès diminue à mesure que le poids augmente, ce qui est assez intuitif. Toutefois, et c'est assez surprenant, pour les bébés de poids très faible, le taux de mortalité est moindre chez ceux dont la mère fumait pendant la grossesse.

Ce graphique est une simple visualisation de probabilités conditionnelles. On représente des taux de décès « sachant que la mère fumait » et « sachant le poids de naissance ». Le danger, avec l'utilisation des probabilités conditionnelles et de la règle de Bayes, est que le « sachant » (décrivant le conditionnement) est souvent interprété de manière causale. Afin de mieux comprendre ces corrélations et ces probabilités conditionnelles, il est important de formaliser le problème. Soit T la variable de tabagisme maternel, et M la variable indicatrice de décès. On observe que les taux de mortalité infantile aux États-Unis sont respectivement, pour une mère fumeuse,

$$\mathbb{P}(M=1|T=1)=\frac{1309}{100000}=1.31\%$$

et pour une mère non fumeuse,

$$\mathbb{P}(M=1|T=0)=\frac{864}{100000}=0.86\%$$

Un indicateur usuel pour comparer les deux risques est le « risque relatif », défini comme le ratio des deux probabilités

$$RR_{M-T}=\frac{\mathbb{P}(M=1|T=1)}{\mathbb{P}(M=1|T=0)}=1.52$$

avec un intervalle de confiance de l'ordre de [1.49 ; 1.57]. On peut aussi étudier le taux de décès en

fonction du tabagisme mais aussi du poids à la naissance. Si l'on se contente d'introduire une variable « poids trop faible » (notée P=1), on peut utiliser un modèle logistique,

$$\log \frac{\mathbb{P}(M=1|T=1)}{\mathbb{P}(M=1|T=0)} =$$

$$\beta_0 + \beta_T \mathbf{1}(T=1) + \beta_P \mathbf{1}(P=1) + \beta_{T-P} \mathbf{1}(T,P=1)$$

À partir de ces probabilités, on peut déduire deux risques relatifs : si le bébé n'est pas de poids trop faible, on retrouve un risque (significativement) plus grand que 1

$$RR_{M-T|P=0} = \frac{\mathbb{P}(M=1|T=1,P=0)}{\mathbb{P}(M=1|T=0,P=0)} = 1.72$$

avec un intervalle [1.65 ; 1.80]

ce qui correspond à notre intuition, et pour les bébés de poids très faible

$$RR_{M-T|P=1} = \frac{\mathbb{P}(M=1|T=1,P=1)}{\mathbb{P}(M=1|T=0,P=1)} = 0.78$$

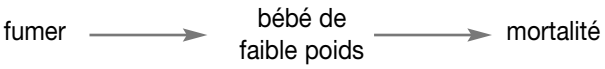
avec un intervalle [0.75 ; 0.80].

Il y a manifestement un paradoxe. Et l'avantage de disposer de tels volumes de données est de pouvoir affirmer qu'il ne s'agit pas d'un bruit statistique. Il y a statistiquement moins de risque de décès si la mère fume.

Utilisation de diagrammes causaux

La difficulté de l'exercice, que connaissent tous les actuaires, est de traduire des informations chiffrées (ici des probabilités de décéder l'année de la naissance) en une langue claire et aussi juste que possible. Les diagrammes causaux, décrits en détail dans Pearl [2000], sont aujourd'hui l'outil principal pour formaliser un tel mécanisme. Par exemple, sur la figure 2, on représente l'idée que l'on se fait de la relation causale : le fait de fumer a une influence sur le poids du bébé, lequel a lui-même une influence directe sur la mortalité. Mais il n'existe pas, dans ce schéma, de lien (direct) entre le fait que la mère fume et la mortalité du nouveau-né. Ce qui devrait se traduire, si ce modèle était juste, par le fait que si l'on considère des enfants de même poids, la probabilité de décès serait la même, que la mère ait fumé ou pas.

Figure 2 - diagramme causal 1



Source : auteurs.

À partir de cette interprétation, on peut tester ce schéma causal avec des données.

$$RR_{M-P|T=1} = \frac{\mathbb{P}(M=1|T=1,P=1)}{\mathbb{P}(M=1|T=1,P=0)} = 11.25$$

avec un intervalle [10.72 ; 11.78]

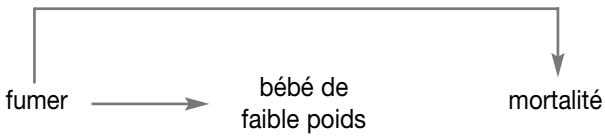
pour les mères fumeuses, alors que pour les mères non fumeuses

$$RR_{M-P|T=0} = \frac{\mathbb{P}(M=1|T=0,P=1)}{\mathbb{P}(M=1|T=0,P=0)} = 24.91$$

avec un intervalle [24.19 ; 25.63].

Ce premier diagramme causal n'est donc pas valide, compte tenu de la différence entre les risques observés : le fait que la mère fume a un impact sur la mortalité. On peut alors envisager une autre relation causale, comme sur la figure 3 : et si la mortalité infantile était en fait uniquement liée au tabagisme de la mère ? Ces diagrammes causaux se traduisent par les mêmes corrélations, mais les mécanismes en jeu ne sont pas du tout équivalents.

Figure 3 - diagramme causal 2



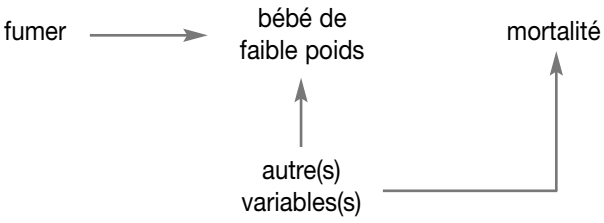
Source : auteurs.

Les données tendent à réfuter cette idée (de causalité indirecte) affirmant que la surmortalité des bébés de faible poids serait en fait liée au fait que la mère fumait.

Recherche de causes communes et prise en compte d'autres variables

En allant un peu plus loin, on peut imaginer aussi qu'il existe des causes communes, autres que le tabagisme, entre le faible poids à la naissance et la surmortalité. Par exemple, figure 3, on peut imaginer un mécanisme causal assez simple. Fumer a un impact sur le poids des bébés (ce point est relativement bien établi par une multitude d'études), mais d'autres variables interviennent aussi (comme la sous-alimentation de la mère ou une malformation congénitale du bébé – pour simplifier, nous retiendrons cette dernière hypothèse).

Figure 4 - diagramme causal 3



Source : auteurs.

Dans ce modèle, un enfant de faible poids à la naissance dont la mère ne fume pas a forcément une malformation congénitale (c'est le principe de ces relations causales) car on a ici seulement deux causes possibles. De plus,

- une malformation congénitale augmente la mortalité infantile ;
- le tabagisme n'augmente pas la mortalité (il affecte juste le poids des bébés).

Avec ce modèle, les bébés de poids faible dont la mère ne fume pas ont alors forcément une maladie congénitale, et donc leur taux de survie diminue. On a alors une relation (corrélation) négative entre le tabagisme de la mère et la mortalité infantile. Et il n'est alors pas impossible d'avoir $RR_{(M-T|P=1)}$ inférieur à 1, comme nous l'avions observé numériquement. Les diagrammes causaux permettent de comprendre ces paradoxes. Mais reste à les tester...

Big data et modèles de médiation

On dispose de plus en plus de gros volumes de données, en particulier sur les naissances. Avec des bases non seulement exhaustives (comprenant ici toutes les naissances recensées) mais de plus en plus détaillées, et énormément d'informations sur la famille, sur l'accouchement, etc. En épidémiologie, des modèles dits de médiation – tenant compte d'informations additionnelles – ont connu un développement important ces dernières années. On peut alors calculer des taux de risques, lorsque la variable de médiation U est binaire. Le principe, dans notre dernier modèle causal, est que seule cette variable U influence la mortalité.

Autrement dit, le facteur de risque

$$RR_{M-U|T,P} = \frac{\mathbb{P}(M=1|T=t,P=p,U=1)}{\mathbb{P}(M=1|T=t,P=p,U=0)}$$

ne doit dépendre ni de t, ni de p. On peut alors tâtonner parmi toutes les variables pour en trouver qui vérifient cette propriété. Il n'est alors pas rare de voir un facteur de risque corrigé, afin de synthétiser l'information. Par exemple, $RR_{M-U|T,P}$ deviendra

$$RR^{\star}_{M-T|P} = \frac{RR_{M-T|P}}{\text{biais}(P)} \quad \text{avec}$$

$$\text{biais}(P) = \frac{1+[\gamma-1]\mathbb{P}(U=1|T=1,P)}{1+[\gamma-1]\mathbb{P}(U=1|T=0,P)}$$

Aller (bien) au-delà de la corrélation

Ces modèles permettent enfin de mieux comprendre les mécanismes causaux, et de mieux cibler les actions de prévention des instituts de santé publique. Et cela est possible grâce aux volumes colossaux de données qui sont aujourd'hui collectés, avec non seulement des bases quasiment exhaustives, contenant énormément d'observations (on retrouve le fameux n = tout le monde de Meyer-Schönberger & Cukier [2013], mais également de plus en plus de variables, souvent bien renseignées. Et si le danger des *spurious regression* rôde (régression fallacieuse, venant du fait que, parmi de nombreuses variables, on peut toujours en trouver deux parfaitement corrélées), la construction et la validation de diagrammes causaux permettent justement d'avoir des interprétations justes.

Denuit [2005] notait que « l'assureur qui désire faire usage d'un critère de segmentation doit pouvoir démontrer, statistiques à l'appui, le lien causal entre ce critère et les variations de la sinistralité qu'il est supposé induire ». Pour l'instant, certaines variables sont utilisées à cause de la corrélation apparente qui existe, et parce que les vrais facteurs de risque (dans le cas du risque automobile, agressivité au volant, non-respect du code de la route, consommation d'alcool, fatigue, etc.) ne sont pas observables et ne peuvent être incorporés dans le tarif. Avoir accès à des données plus fines (et nettement plus volumineuses) permettrait déjà de mieux comprendre les relations causales, et d'envisager d'autres critères de tarification, évitant ainsi l'iniquité inhérente à l'utilisation de variables simplement corrélées avec la sinistralité.

Bibliographie

CDC, bases de données ftp://ftp.cdc.gov/pub/Health_Statistics/NCHS/Datasets/DVS/periodlinkedus/

Charpentier A., « Interprétation, intuition et probabilités », *Risques*, n° 99, septembre 2014.

Denuit M., « Quand la différenciation tarifaire est-elle techniquement justifiée ? », *Le Monde de l'assurance*, dossier spécial, 16-31 mai 2005.

Dubuisson B., « Solidarité, segmentation et discrimination en assurances, nouveau débat, nouvelles questions », 2008, http://goo.gl/LZRFXT.

Hernandez-Diaz S. ; Schisterman E. F. ; Hern MA., "The Birth Weight 'Paradox' Uncovered?", *American Journal of Epidemiology*, n° 164, 2006, pp. 1115–1120.

Meyer-Schönberger V. ; Cukier K., *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Eamon Dolan, 2013.

Pearl J., *Causality: Models, Reasoning and Inference*, Cambridge University Press, 2000.

VanderWeele T. J., "Bias Formulas for Sensitivity Analysis for Direct and Indirect Effects", *Epidemiology*, n° 21(4), 2010, pp. 540-551.

Le partage public/privé du marché de la dépendance

Philippe Caton

Responsable partenariats technologiques, Covéa R&D

Sébastien Nouet

Enseignant-chercheur, Léonard-de-Vinci Pôle Universitaire, Finance Lab

Membre de l'Institut des actuaires (IA)

Michel Revest

Directeur recherche et innovations, Covéa

Le marché de la dépendance ne pourra se développer fortement qu'à travers un système public-privé, similaire sur certains points à celui de la santé ; ceci en fournissant une prise en charge paramédicale grâce à des garanties à la fois assurables et innovantes répondant bien aux besoins des assurés, assurés dont la sinistralité associée est supérieure au tiers au-delà de 85 ans. Deux scénarios de prise en charge privée complémentaire sont proposés dans lesquels les assureurs ont accès à une base de données commune et panélisée afin d'acquérir avec le temps le recul nécessaire à l'observation du risque grâce à un échantillon national de taille importante. La piste principale de la forme financière de l'adossement de la part complémentaire se traduit par la transformation de l'épargne vie en épargne dépendance. Cet article propose ainsi des solutions innovantes afin de développer ce marché et aborde le problème sous-jacent de la prévention.

Lorsque le sinistre survient, c'est-à-dire lorsque l'état de dépendance est déclaré pour l'assuré, l'assureur est dans l'obligation d'honorer son engagement à verser à celui-ci la ou les prestations objet du contrat. Deux types d'indemnisation sont a priori possibles : soit une indemnisation basée sur le principe forfaitaire, soit une indemnisation basée sur le principe indemnitaire. Actuellement, en France, les deux seuls modes de prise en charge existants sont de nature forfaitaire, où l'assuré perçoit un montant d'indemnisation déterminé à l'avance. Le premier est géré en capitalisation par les assureurs avec le versement d'une rente dont le montant est déterminé à la souscription et revalorisable ; le second est géré en répartition par les pouvoirs publics dans le cadre de l'allocation personnalisée

d'autonomie (APA). Malheureusement ces deux modes ne font que se juxtaposer d'un point de vue assurantiel : ils ne sont pas vraiment complémentaires et ne répondent pas bien aux besoins des assurés, qui souhaiteraient la mise en place d'un système similaire à celui de l'assurance santé, avec une prise en charge intégrale des dépenses de soins liées à la dépendance. Mais l'impossibilité pour l'assureur d'estimer sur le long terme le niveau des coûts des sinistres en matière de dépendance, s'agissant d'un risque long voire très long, rend impossible ce type de prise en charge.

Trois approches

L'approche forfaitaire : inadaptée aux besoins

Elle consiste pour l'assureur à verser un capital ou une rente dont le montant est stipulé dans le contrat d'assurance, dès lors que l'état de dépendance est survenu. L'indemnisation sous forme de rente consiste à verser à l'assuré jusqu'à sa mort des arrérages annuels, qui, dans la pratique, constitue un complément nécessaire mais non suffisant à l'APA, de nature forfaitaire elle aussi et gérée par les pouvoirs publics. Cette approche permet ainsi à l'assuré de subvenir en théorie à ses besoins, en finançant ses dépenses liées à l'état de dépendance. Ici l'assureur ne rembourse pas les soins, il verse de l'argent périodiquement, chaque mois ou chaque année, sans droit de regard sur l'affectation de la somme versée à l'assuré, lequel est donc libre de dépenser cette rente comme il le souhaite. Du point de vue de l'assureur, l'approche forfaitaire est satisfaisante car elle est assurable au regard de son expérience de pilotage des portefeuilles dépendance et des études actuarielles réalisées [Deléglise *et al.*, 2009]. Cependant, du point de vue de l'assuré, le montant des rentes dépendance, certes revalorisé chaque année en fonction des performances des placements financiers des assureurs et du taux technique du contrat, est trop faible par rapport aux montants engagés et au reste à charge déduction faite de l'APA, et ce dans le cadre d'une prise en charge correcte de la dépendance. En France, l'approche forfaitaire est actuellement la seule proposée par les assureurs et les pouvoirs publics, mais elle ne permet pas de répondre correctement aux besoins des assurés.

L'approche indemnitaire : non assurable

Cette approche consiste à prendre en charge l'ensemble des dépenses de l'assuré relatives à son état de dépendance, et cela en principe sans limitation, ni du point de vue du montant des dépenses engagées annuellement ni en matière de durée. Dans le domaine de la santé, cette approche est pratiquée aujourd'hui et depuis plusieurs décennies, de manière conjointe par la Sécurité sociale et les mutuelles santé des assureurs, qui remboursent alors des soins de nature médicale et, dans le cadre de la dépendance, les soins paramédicaux associés (soins infirmiers, kinésithérapie, aide à domicile, etc.) ne font souvent pas partie de ce champ d'intervention classique, même si la frontière entre ces deux types de prise en charge est dans certains cas assez difficile à définir. Pour une prise en charge intégrale contre la dépendance qui serait de nature indemnitaire, l'assureur rembourserait alors à l'assuré, à partir de sa date d'entrée en dépendance, l'intégralité des soins paramédicaux dont il bénéficie afin d'accompagner sa perte d'autonomie, et ce jusqu'à sa mort. Cette expérience, tentée aux États-Unis (avec des conditions de compléments assuranciels différentes, puisque le socle de sécurité sociale y est assez limité) dans les années 1990, a conduit à la faillite des deux seules sociétés d'assurance [Cutler, 1993] qui se sont engagées dans cette voie. En effet, si l'anticipation de l'évolution des fréquences d'entrée en dépendance reste relativement correcte, bien que parfois difficile, lorsque les fréquences sont calculées sur des sous-groupes assez larges de population et selon les deux niveaux de dépendance – partielle et totale –, il n'en va pas de même en ce qui concerne l'anticipation de l'évolution dans le temps des coûts des sinistres associés aux états de dépendance dans un contexte de long terme, c'est-à-dire celui d'âges de souscription relativement jeunes tels que 50 ans. C'est ici la

composante coût de sinistre qui est principalement responsable de la non-assurabilité de cette approche dans un contexte de prise en charge de long terme. En effet, Nouet [Nouet et Plisson, 2007] et Cutler [1993] démontrent à partir de données respectivement françaises et américaines que les assureurs sont dans l'impossibilité d'estimer le niveau des coûts de la dépendance et donc celui des prestations associées, et ce à horizon lointain. La commercialisation de produits d'assurance de type indemnitaire qui pourraient répondre correctement aux besoins des assurés est dans les faits impossible pour des raisons d'assurabilité.

L'approche pseudo indemnitaire : la troisième voie

Cette approche, non encore expérimentée en France, consisterait à rembourser des soins soit en fixant un plafond mensuel de remboursement, soit en limitant les remboursements dans le temps. Par exemple, dans ce dernier cas, l'assureur s'engagerait à rembourser l'intégralité des soins de l'assuré mais pendant une période limitée à deux années. Si l'assuré vit trois ans en dépendance, il ne bénéficiera donc pas de couverture pendant un an.

Ou bien on se positionne dans le premier cas de figure, où l'assureur rembourse les soins de manière illimitée dans le temps mais en tenant compte d'un certain plafond de remboursement mensuel. Par comparaison alors avec l'approche forfaitaire, dans la pratique, cette approche se traduit par des montants de prise en charge qui peuvent être importants, donc appréciables pour l'assuré, sans toutefois dépasser un certain plafond, ce qui permet à l'assureur de se couvrir : un produit forfaitaire dont le montant de rente associé serait égal à ce plafond rendrait rédhibitoire sa souscription, car trop coûteux pour l'assuré potentiel. Pour illustration, si l'on considère que 3 000 euros par mois représentent un montant de prise en charge de la dépendance suffisant dans la grande majorité des cas, nous pouvons alors énoncer que la souscription d'un produit forfaitaire versant 3 000 euros par mois à l'assuré en cas de dépendance coûtera substantiellement plus cher à celui-ci que la souscription d'un produit pseudo indemnitaire dont le plafond serait égal au même montant. Cette approche pseudo indemnitaire prend comme point de départ l'approche indemnitaire en matière de coût, approche non assurable pour les âges de souscription relativement jeunes compte tenu de l'imprévisibilité dans le temps des coûts dépendance à long terme mais qui constitue un compromis satisfaisant entre, d'une part, les problèmes d'assurabilité pour les assureurs relatifs à l'évolution du coût des sinistres dans le temps à horizon lointain et, d'autre part, la volonté pour les assurés de se voir proposer par les assureurs une prise en charge de la dépendance adaptée à leurs besoins.

Une troisième voie, de nature pseudo indemnitaire, consisterait à appliquer, de manière supplémentaire, une franchise déduite dans le temps. Dans ce cas-là, l'assureur ne rembourserait pas les soins de prise en charge de la dépendance pendant deux ou trois années, par exemple, années pendant lesquelles l'assuré se couvrirait contre les sinistres de durée raisonnable par l'auto-assurance, puis l'assureur prendrait le relais de la couverture au-delà de cette période. Cette période correspondant à une durée de vie en dépendance calculée sur la base d'un quantile en termes de dépenses cumulées dans le temps, dont le niveau serait de 90 % par exemple, caractérise les sinistres modérés. La déduction assurancielle de cette période éviterait notamment à l'assureur de mutualiser aux premiers euros, avec des coûts d'expertise associés importants au global, et permettrait aux assurés à revenus modestes non seulement de se couvrir à des tarifs plus avantageux mais de se couvrir en beaucoup plus grand nombre auprès des assureurs.

La prise en charge des personnes dépendantes pose la question de l'individualisation des besoins [Revest, 2014] et notamment du maintien à domicile, dont la mise en œuvre peut s'imbriquer dans cette troisième voie. Cela à travers la proposition de services dont le niveau de gamme (qualité du service hôtelier, par exemple) dépendrait du choix de l'assuré et des contraintes de son environnement pour la prise en charge à domicile : à perte d'autonomie objectivement identique du point de vue médical (même

classement selon la grille Aggir), les besoins de services et d'aide financière peuvent être très différents d'un individu à l'autre.

Quelles solutions pour les assureurs

Une prise en charge garantie par l'assureur

Les assureurs devront couvrir la dépendance dans le cadre d'un système de remboursement similaire à celui de l'assurance santé, et de manière complémentaire à la prise en charge des soins dépendance par la sécurité sociale. Ceci étant possible par exemple, grâce à une cinquième branche de la Sécurité sociale ou un système équivalent public-privé. Ce système s'appuierait d'un point de vue technique, en ce qui concerne le suivi du risque et son estimation, sur une base de données dépendance panélisées. La question est de savoir si ce système serait géré, pour sa part complémentaire, en répartition ou en capitalisation, et sous quelles formes.

L'approche purement indemnitaire, gérée en capitalisation, n'est pas envisageable dans la majorité des cas, à l'exception des âges de souscription relativement avancés, soit environ 75 ans, car alors l'évolution des coûts est prévisible. Si le risque dépendance est géré en capitalisation par les assureurs (complémentairement à la Sécurité sociale), l'approche pseudo indemnitaire se révèle comme étant la seule approche assurable couvrant relativement bien les besoins des assurés pour la majorité des âges de souscription, c'est-à-dire inférieurs à 75 ans. Si le risque est géré en répartition par les assureurs (complémentairement à la Sécurité sociale), l'approche indemnitaire pure ne peut être appliquée (à l'ensemble des âges de souscription) qu'à une condition, assez contraignante et difficile à mettre en place : celle de la souscription obligatoire pour l'ensemble de la population française (de plus de 60 ans, par exemple), car dans ce cas l'assureur pourra réajuster ses tarifs au fur et à mesure de son observation du risque avec ses déviations possibles alors prises en compte en continu dans le pilotage du portefeuille. C'est le premier schéma de prise en charge, avec une gestion en capitalisation et une approche pseudo indemnitaire, qui apparaît comme le plus réaliste.

Voyons maintenant les modalités de prise en charge associées aux deux solutions qui viennent d'être exposées.

L'adossement de produits dépendance

Les assureurs doivent se poser les deux questions suivantes : quels produits assuranciels se prêtent le mieux à l'adossement de produits dépendance et comment procéder à cette adaptation des contrats ? Les produits d'assurance candidats à cet adossement sous plusieurs formes sont : les produits santé, les garanties des accidents de la vie (GAV), l'épargne vie, les multirisques habitation (MRH) et l'assurance automobile. À noter que, pour des raisons techniques et pratiques, ces types de contrats peuvent favoriser une meilleure prise en charge de la dépendance du fait d'une meilleure identification du risque, grâce notamment aux produits santé, ainsi qu'une implication plus importante de l'assureur dans le domaine de la prévention [Pôle Finance Innovation, 2013], par exemple avec la MRH (état des lieux et adaptation du logement du senior afin de prévenir les accidents de la vie conduisant à la perte d'autonomie).

Les formes financières de l'adossement pourraient se traduire soit par une taxe sur un sous-ensemble de ces produits afin de financer un fonds de garantie dépendance qui pourrait voir le jour par décision des pouvoirs publics si les assureurs n'innovent pas, soit par la transformation de l'épargne vie en garantie dépendance sur décision des assureurs [Pôle Finance Innovation, 2013].

Concernant les formes assurancielles au sens propre, l'adossement de ces produits peut se traduire par la mise en place :

• soit d'une « GAV dépendance », qui implique la proposition d'un nouveau produit collectif géré en répartition par les assureurs avec souscription obligatoire et tarifs révisables, ce qui ouvrirait la voie à une offre de garanties sous une forme pseudo indemnitaire ou indemnitaire ;

• soit d'un produit d'assurance vie impliquant une sécurisation de l'épargne sans couverture dépendance avant 65-75 ans, car cette période correspond à une faible voire très faible sinistralité et sert donc l'intérêt commercial de l'assureur. Ce produit revêt alors les deux formes possibles suivantes :

– une assurance vie avec sortie à 65 ans en rente dépendance en cas de sinistre sous une forme forfaitaire voire pseudo indemnitaire (indemnitaire plafonnée) par le paiement à cet âge en prime unique au moyen d'un bien immobilier ou d'un plan d'épargne retraite populaire (Perp),

– une assurance vie avec sortie à 75 ans en garantie pseudo indemnitaire voire indemnitaire en cas de sinistre par le paiement à cet âge en prime unique au moyen d'un bien immobilier ou d'un Perp, la forme non forfaitaire étant possible en raison de la prévisibilité des coûts de la dépendance à moyen terme, c'est-à-dire jusqu'à la date de la mort, ici pas très éloignée.

Complément relatif à la prévention

Un sujet transversal est celui de la prévention de la dépendance [Pôle Finance Innovation, 2013], vue sous l'angle de la prise en charge à domicile, que les principaux acteurs concernés, en particulier les assureurs et la profession paramédicale, doivent veiller à rendre satisfaisante.

Même si les assurés sociaux sont inégaux devant la maladie, la préparation de la période de la retraite par les différents acteurs de l'assurance doit s'effectuer à l'échelle de la population française. Le développement et la maturité des technologies de l'information et de la communication (TIC) permettent des avancées très importantes en matière de maintien et d'autonomie à domicile, et, depuis quelques années, l'avènement de la santé qualifiée de « connectée » et du concept de la « quantification de soi » (*Quantified self*), importé des États-Unis en 2007, contribuent en ce sens aux processus d'innovation dans le domaine de la santé.

D'une manière plus large, cette santé « connectée », ou en quelque sorte ce « bien-être connecté », grâce à des dispositifs impliquant des capteurs corporels, permet pour la première fois aux individus (robustes, fragiles, jeunes ou âgés) de mieux apprécier leurs interactions avec leur environnement, de mesurer en temps réel l'impact de leurs modes de vie (activité physique, nutrition, comportements, etc.) sur leur organisme, et ce d'une manière simple, ludique, peu coûteuse, avec des objets fiables et simples d'utilisation, avec comme support principal le smartphone et le Web ou avec des outils accessibles à tous. Il s'agira de convertir l'engouement pour les objets connectés en volonté d'utiliser des instruments de gestion de la santé pour les personnes fragiles, voire prédépendantes et dépendantes. Dans un cadre paramédical mis en place en accord avec les patients, les médecins, voire avec les assureurs, nous pouvons constamment autoévaluer, suivre, mesurer, adapter, enregistrer et éventuellement partager les données pour corriger, prévenir de manière quasi prédictive toute anomalie pouvant perturber l'état de santé de l'utilisateur.

Concept adaptable à l'ensemble de la population, la richesse informative apportée par les données recueillies permettra au niveau de l'assureur l'individualisation des conseils, voire par la suite leur personnalisation via le corps médical. La santé « connectée » est un outil de prévention universel privé-public à destination :

• des personnes en pleine santé, quel que soit leur âge, afin de leur faire adopter les bonnes pratiques, de cerner leur mode de vie et ses impacts potentiels sur le plan médical pour préserver leur bon état de santé ;

• des personnes préfragiles ou fragiles, afin de réaliser un suivi plus régulier des évolutions, d'anticiper, d'adapter, de corriger en fonction des résultats pour ralentir le basculement d'un stade à un autre plus avancé et reculer la survenance de la perte d'autonomie ; à titre d'illustration, chez les préfragiles, notamment chez les personnes atteintes de maladies chroniques, la santé connectée se traduira par la mesure, la prévision et par des alertes adaptées pour faciliter leur vie quotidienne ;

• des personnes dépendantes, afin de les accompagner, de les suivre, de les évaluer plus régulièrement et plus facilement (en évitant les déplacements inutiles, par exemple), d'adapter les traitements, tout cela grâce à un environnement paramédicalisé s'appuyant du point de vue technologique sur le recueil de données via des capteurs destinés à la protection des biens et des personnes, et qui permet de rompre l'isolement ;

La santé « connectée » permettra au fil des années d'encourager les bonnes pratiques et de préparer les personnes à aborder l'avancée en âge dans les meilleures conditions, et ce le plus tôt possible. La mise en œuvre de la prévention devrait permettre de faire baisser les fréquences associées à la survenance des pathologies, et notamment celles des pathologies chroniques, de faire reculer la préfragilité ou la fragilité en lien avec les états de survenance de la dépendance, d'améliorer le partage entre public et privé des coûts de la santé. Avantageuse pour la santé publique, la santé « connectée » devrait induire des modifications de comportements, offrir des moyens d'analyser des cohortes significatives à moindre coût, modifier les relations assureur-client et médecin-patient. Elle peut être vue comme l'un des futurs outils de la réforme de la santé. Le consensus entre les différents acteurs publics et privés permettra d'amorcer et d'entretenir les processus d'innovation spécifiques à ce domaine. Dans ce cadre, les questions soulevées sont les suivantes :

• Quel sera le rôle de l'assureur ? Celui d'un organisme classique de prise en charge ou celui d'un organisme jouant de manière complémentaire un rôle de prévention avec des intéressements financiers prenant la forme d'économies futures, cela grâce aux nouveaux apports de la santé digitale.

• Comment encadrer juridiquement la collecte des données et, concrètement, comment convaincre nos clients de communiquer anonymement leurs données ?

• Comment rendre plus sociale l'image de l'assureur auprès des assurés afin de créer un marché d'autant plus large de la santé digitale ? Par la pédagogie ? En montrant notre implication majeure dans la vie quotidienne du citoyen et de la collectivité ? Par notre éthique et notre transparence sur la bonne utilisation de ces données, données destinées à l'amélioration de la santé de chacun pour l'équilibre et l'harmonie de notre société ? Par la prise de conscience de la nécessité de consacrer une place plus importante à la médecine préventive et réduire ainsi les coûts de la santé pour les assureurs et les assurés ?

Conclusion

La seule approche possible en matière de prise en charge de la dépendance est de nature pseudo indemnitaire, approche à la fois assurable et satisfaisante pour les assurés, Les soins paramédicaux seraient en partie pris en charge par une cinquième branche de la Sécurité sociale ou un système équivalent, et en partie par une part complémentaire associée et plafonnée par l'assureur qui serait vraisemblablement gérée en capitalisation. Le risque financier relatif à la dépendance pour l'assuré est moins la survenance de la perte d'autonomie que la durée de l'état de dépendance, l'incertitude liée à celle-ci constituant un facteur d'inégalité et de risque parmi les assurés. Dans le cadre d'une prise en charge pseudo indemnitaire, une des pistes novatrices en termes de couverture serait l'introduction de franchises exprimées en années, la prise en charge de l'assureur intervenant au-delà d'un certain montant ou d'une certaine durée de l'état de dépendance. De manière connexe, en ce qui concerne le financement de la couverture, la piste

novatrice serait la transformation d'une partie de l'épargne vie en épargne dépendance.

Les assureurs et les organismes mutualistes se positionnent aujourd'hui non seulement comme des acteurs incontournables dans les domaines de la prévoyance, de la retraite et plus spécifiquement dans celui de la dépendance, mais ont vocation à occuper une place de plus en plus importante dans la vie sociale compte tenu des facteurs majeurs combinés et grandissants que sont le phénomène de vieillissement et les réformes structurelles sociales et économiques qui conduisent, pour ces dernières, au désengagement de l'action publique dans la couverture sociale de base.

Les assureurs et les mutuelles doivent alors faire face à certains enjeux majeurs classiques, comme celui de la retraite, mais aussi s'ouvrir davantage au chantier de la couverture dépendance, dont les attentes en matière de prise en charge sont de plus en plus nombreuses. L'assurance dépendance proprement dite, celle des contrats à fonds perdus de la branche prévoyance, n'est qu'un outil dans une stratégie financière plus globale impliquant toute une panoplie de solutions et de produits. Aussi, les assureurs et les mutuelles pourront jouer un rôle plus important dans les assurances sociales, dont relèverait l'assurance dépendance, grâce à l'instauration de règles de mutualisation et de sélection des risques saines, tout en étant capables de satisfaire de manière élargie aux besoins des assurés sociaux.

Afin de répondre favorablement à ces attentes, les assureurs ont à leur disposition des leviers assuranciels de prise en charge du risque et d'adossement des produits mis en avant dans cet article. La mise en pratique de ces leviers devra s'inscrire dans le cadre d'une collaboration constructive avec les pouvoirs publics et les organismes paritaires.

Bibliographie

Cutler D., "Why Doesn't The Market Fully Insure Long-Term Care?", Working Paper n° 4301, NBER, mars 1993.

Deléglise M.-P. ; Hess C. ; Nouet S., « Tarification, provisionnement et pilotage d'un portefeuille dépendance », *Bulletin français d'actuariat*, n° 17, 2009, pp. 70-108.

Finance Innovation, « L'innovation dans le domaine de la "longévité bien vieillir" », synthèse du groupe de travail « Longévité – bien vieillir » dirigé par M. Revest, Livre blanc de l'assurance n° 2 « L'innovation dans l'assurance au pôle Finance Innovation : restitution de travaux », partie 2, Pôle Finance Innovation, 2013. Disponible en PDF : *http://www.finance-innovation.org/files/part_2_longevite_bien_vieillir.pdf*

Nouet S. ; Plisson M., « L'assurabilité de la garantie indemnitaire du risque dépendance », *Risques*, n° 71, septembre 2007.

Revest M., Éditorial *Newsletter LAB*, Laboratoire Assurance Banque, « Chaîne de valeur et rôle social de l'assurance », juin 2014, *http://www.cerclelab.com/les-newsletters-du-lab/107-eletter/1186-2014-06-edito-revest.html*

Actualité de la Fondation du risque

La crise accroît-elle la peur du risque ? (1)

Luc Arrondel (2)

Membre de la chaire « Transitions démographiques, transitions économiques »

Les Français investissent de moins en moins en bourse, préférant des placements plus sûrs, comme le livret A. Cette évolution s'est accentuée depuis les crises successives des subprimes et des dettes souveraines. Est-ce à dire que la crise rend les épargnants plus averses au risque ? Sinon, comment expliquer les modifications des comportements financiers ? Luc Arrondel et André Masson ont analysé ces évolutions, grâce à une grande enquête menée entre 2007 et 2011 (Cf. encadré méthodologie p. 132).

Depuis la chute de Lehmann Brothers, les Français font preuve de plus de prudence dans leurs placements financiers. Une série d'enquêtes (Pater), réalisées entre 2007 et 2011, a mesuré l'évolution des comportements. Le nombre d'actionnaires déclarés a ainsi diminué de 40 % entre décembre 2008 et juin 2012, tandis que les dépôts sur le livret A ont progressé d'environ 30 % (3). Les ménages eux-mêmes se déclarent plus prévoyants. À la question « Diriez-vous que depuis la crise financière vous êtes devenus plus prudent, moins prudent, ou vous n'avez pas changé ? », 48 % des personnes interrogées se disaient plus précautionneuses en 2009. Cette proportion est montée à 54 % en 2011, même si ces évolutions doivent être nuancées selon les différentes catégories sociales de la population.

Face à ces constats, il est tentant de conclure que la crise rend les particuliers plus averses au risque. Mais cette conclusion n'est-elle pas un peu rapide ? Existe-t-il d'autres facteurs explicatifs à ces changements d'attitude ? Grâce à cinq vagues d'enquêtes, Luc Arrondel et André Masson ont étudié l'impact de la crise sur les comportements patrimoniaux des

Français. Ils ont analysé les évolutions en matière d'épargne au cours du temps et ont cherché les facteurs explicatifs de ce changement.

Les constats de l'enquête

Trois facteurs clés

Les choix en matière d'épargne dépendent de trois grands types de facteurs. Tout d'abord, les « ressources » disponibles de l'individu. Il s'agit évidemment de son patrimoine mais aussi de son capital santé, son niveau d'éducation, ses connaissances financières…

Ensuite, la perception de l'environnement et les anticipations vis-à-vis du futur. Cette catégorie regroupe des éléments économiques (évolution de salaire, risque de chômage, montants de la future pension de retraite…), tout comme les anticipations en matière d'état de santé ou d'espérance de vie, voire celles concernant les évolutions du système de protection sociale.

Enfin, les préférences de l'individu à l'égard du risque et du temps. Ces facteurs renvoient au degré d'aversion au risque et à la préférence pour le présent (la façon dont un individu pondère le bien-être futur par rapport à son bien-être présent). Les préférences de l'épargnant influent en effet sur les arbitrages entre consommation et épargne.

Une mesure du risque controversée

Un des points régulièrement discutés dans la littérature académique est la mesure de l'aversion au risque. Traditionnellement, les études l'évaluent via des critères quantitatifs, comme les échelles de risque à la Likert (sur une échelle de 0 à 10, la personne auto-évalue sa propension à prendre des risques), ou via des questions sur des choix d'investissements financiers virtuels. La méthode de *scoring* utilisée par les chercheurs est différente puisqu'elle inclut des mesures qualitatives afin de dessiner un « portrait psychologique » de l'épargnant. Via des questions portant sur les différents aspects de la vie (consommation, travail, sport, etc.), les auteurs évaluent les préférences des sondés à l'égard du risque et du temps.

Des préférences identiques

Les résultats de l'enquête montrent que, pour une majorité de ménages, les ressources disponibles étaient encore peu touchées par la crise en 2011. La baisse des revenus ne peut donc pas justifier les changements des comportements financiers. L'explication vient-elle, dans ce cas, d'une plus grande allergie au risque ? Les méthodes de mesures traditionnelles, souvent sensibles à l'environnement économique, vont dans ce sens puisqu'elles indiquent une augmentation de l'aversion relative au risque. Mais les « scores », mis au point par Luc Arrondel et André Masson, donnent une vision contradictoire.

Méthodologie

Débutée en 1998 par l'Insee, l'enquête Pater (Patrimoine et préférences vis-à-vis du temps et du risque) a été relancée par Luc Arrondel et André Masson en 2007. Plus de 3 600 ménages ont été interrogés. Outre l'information recueillie habituellement dans les enquêtes patrimoniales, Pater met l'accent sur les questions qualitatives et subjectives visant à mesurer les préférences de l'individu en matière d'épargne (aversion au risque, préférence pour le présent, altruisme…), ainsi que les anticipations concernant ses ressources futures.

Les préférences de l'individu sont ainsi mesurées par une méthode originale de *scoring* [Arrondel et Masson, 2014] à partir de loteries, mais aussi en fonction des attitudes, des opinions, des comportements dans différents domaines de la vie (santé, professionnel, loisirs, consommation, retraite…).

Selon cet outil, les épargnants ont toujours la même attitude à l'égard du risque. Ils sont globalement aussi tolérants qu'avant la crise : « ni plus, ni moins », indique l'étude. Quant à la préférence temporelle, elle est également restée stable : le goût pour l'épargne n'a guère évolué.

Mais des anticipations plus pessimistes

La nouveauté est ailleurs, dans la perception de l'avenir. Les individus sont devenus beaucoup plus pessimistes, en particulier après la crise des dettes souveraines de 2011. Ils revoient leurs anticipations à la baisse : alors que les personnes interrogées tablaient sur une progression de leurs revenus de 3 % en 2007, elles anticipaient une stagnation en 2011. De même, le rendement moyen anticipé sur le marché boursier passe de 5,6 % en 2007 à 0 % en 2011. Plus pessimistes à l'égard de la bourse, les Français s'en éloignent…

Recommandations

La question de l'orientation de l'épargne vers des investissements de long terme est régulièrement au cœur des débats politiques. L'étude présentée permet de voir quels leviers peuvent être utilisés pour influencer les choix des épargnants.

S'il est très difficile de changer le degré d'aversion au risque des individus, les pouvoirs publics peuvent intervenir afin de sécuriser l'environnement, et rassurer ainsi les épargnants.

Garantir la pérennité du système de retraite, assurer la stabilité de la politique fiscale, sont autant d'éléments qui contribuent à une perception optimiste de l'avenir.

La plus grande prudence des épargnants dans leurs placements financiers s'explique ainsi par leur perception plus sombre de l'environnement économique, et non par un changement des préférences vis-à-vis du risque. Pourquoi investir dans des actions si on est persuadé qu'elles ne rapporteront rien ? La vision plutôt noire du contexte économique serait, pour les auteurs, la première cause du rejet des produits risqués. Reste donc à redonner un peu d'optimisme à la population. S'il est en effet très difficile d'influencer le degré d'aversion au risque d'un individu, des mesures pourraient être prises afin de sécuriser l'environnement économique, fiscal et social.

À retenir

Depuis la crise de 2008, les Français se montrent beaucoup plus prudents dans leurs placements financiers. Ils délaissent la bourse au profit des livrets d'épargne, plus sécurisés.

Les particuliers ne sont pas devenus plus averses au risque pour autant. Ils se montrent par contre plus pessimistes.

Anticipant des rendements moindres pour les actions, ainsi qu'une stagnation de leurs revenus, les ménages ont modifié leurs comportements en conséquence.

Notes

1. D'après l'article de Luc Arrondel et André Masson « Mesurer les préférences des épargnants : comment et pourquoi (en temps de crise) ? », et un entretien avec Luc Arrondel.

2. Directeur de recherches au Centre national de recherche scientifique (CNRS), chercheur et professeur associé à l'École d'économie de Paris (PSE – Paris School of Economics). Il est également consultant scientifique à la Banque de France.

3. Source : étude trimestrielle SoFia réalisée par Tns-Sofres auprès de 12 000 panelistes (dont ceux des enquêtes Pater).

Bibliographie

ARRONDEL L. ; MASSON A., « Mesurer les préférences des épargnants : comment et pourquoi (en temps de crise) ? », *Économie et Statistique*, n° 467-468, 2014, pp. 5-49.

BORGHANS L. ; DUCKWORTH A. L. ; HECKMAN J. J. ; TER WEEL B., "The Economics and Psychology of Personality Traits", *Journal of Human Resources*, n° 43(4), 2008, pp. 972-1059.

BARSKY R.B. ; KIMBALL M.S. ; JUSTER F.T. ; SHAPIRO M.D., "Preference Parameters and Behavioral Heterogeneity: An Experimental Approach in the Health and Retirement Survey", *Quarterly Journal of Economics*, n° 112(2), 1997, pp. 537-580.

DOHMEN T. ; FALK A. ; HUFFMAN D. ; SUNDE U. ; SCHUPP J. ; WAGNER G., "Individual Risk Attitudes: New Evidence from a Large, Representative, Experimentally, Validated Survey", *Journal of the European Economic Association*, n° 9(3), 2011, pp. 522-550.

GUISO L. ; SODINI P., "Household Finance: An Emerging Field", CEPR Discussion Papers n° 8934, C.E.P.R. Discussion Papers, 2012.

Livres

Alexandre Laumonier

6/5

Zones sensibles Éditions, 2014, 250 pages

Comme l'indiquent le titre et son auteur, ce livre est une curiosité à plusieurs égards : il est composé de deux parties, dont une (celle numérotée 6) parut en 2013, avant d'être adjointe à celle publiée en 2014 (numérotée 5). Jusque-là rien d'extraordinaire. Ce qui l'est plus est que ces deux parties sont imprimées tête-bêche. Autrement dit, on peut lire les deux parties de ce livre dans n'importe quel ordre, elles sont indépendantes, à condition d'inverser la position de lecture. Elles traitent toutes deux d'un même sujet, l'évolution des marchés boursiers, tant du point de vue historique que du point de vue technologique. Autre curiosité, le véritable auteur en chair et en os se cache derrière une énigme. La première page affirme que le livre a été écrit par un algorithme, comme ceux qui transmettent et exécutent les ordres des *traders* à Basildon dans la banlieue de Londres, où sont regroupés les serveurs des principaux marchés boursiers. Nous révèlerons l'auteur à la fin, car nous avons eu du mal à le démasquer. D'ailleurs, comme pour brouiller encore plus les pistes, l'algorithme affiche les deux noms de ses prétendus traducteurs, puisque (dit-il) il a fallu traduire en français la suite de 0 et de 1, formant la base binaire du codage des algorithmes.

Passé ce qui ressemble à un canular, la lecture des deux parties révèle que l'auteur connaît très bien le fonctionnement des marchés actuels et leur évolution à sens unique depuis le XIX^e^ siècle, à savoir l'augmentation vertigineuse de la vitesse de transmission des ordres, depuis le télégraphe morse jusqu'aux ordinateurs et leurs algorithmes les plus performants, qui frôlent la limite relativiste de la vitesse de la lumière (30 cm par nanoseconde). Le livre montre clairement, sans jargon, comment les énormes gains de productivité permis par la technologie actuelle ont profité aux marchés (volumes des transactions, vitesse de réaction aux informations, coûts de transaction, etc.) mais aussi aux intermédiaires, les *traders*, qui les manipulent (au sens commun comme au sens juridiquement condamnable) sans que les investisseurs s'en rendent compte. De nombreux exemples décrivent avec minutie les manipulations possibles, certaines encore impunies, pour autant qu'on dispose d'un matériel performant, des logiciels mis à jour et surtout d'une proximité physique des serveurs, comme à Basildon, limite relativiste oblige. La lecture de cette partie (6), intitulée « Le soulèvement des machines », est quelque peu déprimante pour l'espèce humaine car elle accrédite l'idée d'une disparition totale des intermédiaires humains, remplacés par des machines, beaucoup plus rapides et infatigables. L'autre partie (5) procède à l'inverse. Il ne s'agit plus de machines mais d'une galerie de portraits de personnes remarquables (des *people* ?) qui ont marqué l'histoire des marchés d'actions, d'obligations, de matières premières et de leurs marchés dérivés, comme celui des options négociables. Plusieurs de ces personnes sont devenues célèbres pour leur contribution à la théorie financière (citons Fischer Black et Myron Scholes, pères de la célèbre formule d'évaluation des options) ou pour leurs méfaits comme Bernard Madoff, qui fut aussi président du Nasdaq. Ce cas, exemplaire à bien des égards puisqu'il fut la plus grosse escroquerie jamais découverte sur un marché financier et qui passa sous les radars des régulateurs avant d'être tardivement révélée, montre que la limite entre l'innovation audacieuse et le passage à l'acte délictueux est très floue et qu'elle a pu être franchie en toute impunité, faute d'une régulation adaptée aux technologies de pointe.

Un livre agréable à lire, indispensable pour tous ceux qui veulent comprendre le *trading* à haute fréquence et pour tous les régulateurs qui voudraient

l'encadrer, d'une part pour éviter le retour de krachs dus à l'emballement des machines, d'autre part pour que les gains de productivité ne soient pas accaparés par les intermédiaires. Quant à son auteur humain, il faut chercher son nom vers la page 120, à la fin des remerciements, donc au milieu du livre. Surprise ! Il ne s'agit pas d'un *trader* repenti, ni d'un économiste, ni d'ailleurs d'un professionnel de la finance mais d'un chercheur en anthropologie : Alexandre Laumonier, fondateur des éditions Zones sensibles. Comme quoi, un regard extérieur à une profession, le *trading*, voit mieux son intérieur que bien des professionnels.

Par Daniel Zajdenweber

Alain Desroches, Alain Leroy, Frédérique Vallée

***La gestion des risques, principes et pratiques* (3e édition)**

Éditions Lavoisier/Hermès, 2015, 312 pages

L'éditeur Lavoisier s'est imposé comme un spécialiste de la gestion des risques avec plus de 45 titres sur le sujet réunis dans une collection « Sciences du risque et du danger », toutefois le présent ouvrage est antérieur à cette série et provient du fonds d'Hermès. Qu'y trouve-t-on ? Un premier chapitre relatif aux « concepts préliminaires » constitue une approche élégante de l'objet où le risque apparaît comme la conséquence d'une activité « ne pouvant "justifier" de rester pendant toute sa durée dans la zone de certitude ». C'est donc autant par des actions appropriées sur les opérations que par la recherche scientifique qu'on réduit le risque dans cette approche qui se donne comme une philosophie pratique de la science classique. À l'appui de leur démarche, les auteurs emploient le calcul des probabilités qu'ils introduisent en citant de Finetti, Morlat et Savage, sans pourtant engager le lecteur aux hardiesses du subjectivisme : « il est absurde de chercher à probabiliser l'inconnu » (p. 25). Plus que pour le risque ou pour l'incertitude, les auteurs marquent donc une « aversion pour l'inconnu » qu'ils proposent de réduire à un niveau (socialement) acceptable.

Ce premier chapitre présente l'essentiel des méthodes de management des risques qu'on trouve ailleurs, en particulier « l'analyse préliminaire des risques » est introduite comme une évidence : le classement des risques par vraisemblance et par gravité puis la définition d'une échelle de criticité permettent de constituer un référentiel de décision et d'agir sur les principaux risques. Les auteurs passent rapidement sur ce qui constitue la matière principale des cours d'introduction au management des risques, en effet ils visent à la « sûreté de fonctionnement » qui exige évidemment des développements ultérieurs en matière de mesure. À cette fin, un chapitre méthodologique fait la part belle à l'analyse des systèmes (diagrammes de fiabilité, arbres des défauts) et à la quantification (graphes de Markov, réseaux de Petri, etc.). Ces méthodes sont présentées avec le numéro de la norme CEI correspondante : cette référence à la Commission électrotechnique internationale trahit l'expertise industrielle des auteurs, de même que leurs nombreux exemples et la construction même de l'ouvrage.

Après cette présentation des méthodes, il apparaît rapidement que le livre est ordonné autour des exemples rencontrés par Alain Desroches dans l'industrie spatiale et par Alain Leroy dans l'industrie pétrolière. Suivant l'ordre logique de création d'un système, les auteurs expliquent la démarche de gestion des risques projet et celle de la maîtrise des risques industriels pour terminer par la constitution d'un retour d'expérience pour maîtriser la qualité. Deux chapitres séparés traitent des risques informatiques et financiers. Si les premiers bénéficient de l'expérience d'un expert consultant qui présente leur spécificité (en particulier les risques d'intrusion, mais aussi une série de risques des projets liés à la rédaction du cahier des charges) et sont illustrés par des exemples industriels, les seconds sont perçus de manière purement résiduelle. Le paragraphe sur l'assurance illustre la rapidité des démonstrations : « C'est l'existence des grands sinistres qui justifie le recours à l'assurance […] L'ensemble des entreprises ne recouvrera donc, au maximum, que 60 % du montant des primes versées, et n'a donc pas intérêt en moyenne à se couvrir contre des risques de fréquence » (p. 249).

Comme le montre ce dernier exemple, le propos des auteurs est volontiers elliptique. Est-ce parce qu'il s'adresse aux ingénieurs de l'École centrale Paris, premiers bénéficiaires des enseignements d'Alain Desroches, et réputés pour leur esprit délié ? L'interprétation des nombreux schémas comme des exemples repose sur l'autonomie du lecteur qui doit posséder une honnête culture scientifique pour bénéficier des enseignements de ce livre. Sous cette condition, la lecture est rapide, agréable et fort utile : les travaux récents de l'auteur principal [Desroches et Gatecel, 2006] montrent que la méthode s'applique bien au-delà de l'industrie, par exemple aux établissements de santé. À défaut d'une aisance relative avec le calcul des probabilités appliqué, le lecteur aura certainement besoin d'un ouvrage plus explicite.

Par Pierre-Charles Pradier

Bibliographie

Desroches A. ; Gatecel C., « L'analyse préliminaire des risques : un outil adapté aux établissements de soins ». *Risques et qualité en milieu de soins*, vol. III, n° 3, septembre 2006, pp. 141-150.

5.

Remise du prix Risques 2015

et présentation du numéro 100

Présentation par Pierre Bollon

Membre du comité éditorial de *Risques*

Lauréats 2015

Antoine Lefébure et Gérald Bronner

Le 3 février 2015 la revue *Risques* a célébré la parution de son 100e numéro et décerné son prix 2015.

Prononçant quelques mots d'accueil chaleureux, ***Bernard Spitz***, président de la FFSA, se réjouit que la parution du 100e numéro de *Risques*, réalisé sous la direction de Jean-Hervé Lorenzi – qui préside son Comité éditorial – et la remise du prix Risques 2015 soient l'occasion de réunir à la Maison de l'assurance un grand nombre d'amis de notre profession.

Il rend hommage aux créateurs de *Risques*, en particulier ***Denis Kessler*** et ***François-Xavier Albouy***, qui ont eu le sens de ce qui importe, c'est-à-dire de laisser une trace permettant au monde de l'assurance, dépositaire de la gestion du risque, d'élaborer et d'exprimer une pensée autour de sa mission. La présence d'***Éric Lombard***, qui préside l'Université de l'assurance, montre si besoin était qu'il y a dans notre profession une continuité, qui fait sa noblesse, dans ce désir de réflexion et de dialogue. Le numéro 100 de *Risques*, par la diversité et la richesse des témoignages qu'il rassemble, illustre bien le fait que l'assurance est intimement liée à notre société tout entière, à la culture, à la philosophie, au sport, au financement de l'économie, à la protection sociale, à l'entreprise, à la vie politique… La remise par ***Thierry Derez*** du prix Risques 2015, décerné par le jury interdisciplinaire présidé par ***Daniel Zajdenweber***, en fournira d'ailleurs une preuve supplémentaire.

Jean-Hervé Lorenzi rappelle ensuite que la revue est non seulement accueillie mais aussi soutenue en permanence par la FFSA et l'ensemble de la profession. Le Comité éditorial s'attache à ce que *Risques*, trimestre après trimestre, contribue utilement à la réflexion sur la conception et la maîtrise du risque dans les années qui viennent, transcendant, point important, l'opposition traditionnelle entre « risquophobes » et « risquophiles ».

Il donne ensuite la parole à plusieurs des auteurs du ***numéro 100***, qui font à notre revue l'honneur et l'amitié d'accepter d'ajouter leur témoignage oral à leur contribution écrite. ***Nicolas Seydoux, Denis Kessler, Marie Ekeland, Philippe Houzé, Jérôme Grivet, Éric Lombard*** et ***Claudie Haigneré*** soulignent ainsi successivement ce qui leur paraît central dans leur réflexion sur le risque et son appréhension pour notre société, aujourd'hui et dans vingt ans.

Jean-Hervé Lorenzi les en remercie chaleureusement, appelant à lire avec attention ce qu'ils ont écrit, avec 94 autres personnalités, dans le numéro 100. Ce recueil exceptionnel de points de vue nous incite à continuer collectivement à prendre des risques : « Vive le risque » nous a dit ***Nicolas Seydoux*** ! Il passe ensuite la parole à Daniel Zajdenweber qui a accepté de présider cette année le jury du prix, issu du Comité éditorial de notre revue.

Daniel Zajdenweber rappelle comment a travaillé le jury du prix Risques 2015, sélectionnant les deux lauréats après avoir constitué une liste de travaux parus pendant l'année écoulée et portant sur l'intelligence et la compréhension du risque, toutes disciplines confondues.

Le choix du jury pour le **trophée d'or** s'est porté cette année sur le livre d'***Antoine Lefébure***, *L'affaire Snowden, comment les États-Unis espionnent le monde*, qui illustre parfaitement un risque important aujourd'hui, celui de despotisme cybernétique. Le prochain numéro de la Revue sera d'ailleurs en partie consacré aux risques cybernétiques. Le jury a décidé aussi de décerner le **trophée d'argent** à l'ouvrage de ***Gérald Bronner***, *La planète des hommes, réenchanter le risque*, qui nous alerte avec une grande force de conviction sur les usages et effets pervers du principe de précaution, thème d'ailleurs très présent dans notre numéro 100, comme il l'a été dans les interventions précédentes.

Avant de remettre les prix aux deux lauréats, ***Thierry Derez***, président de Covéa, prononce quelques mots sur le thème que le jury lui a soumis : « Pourquoi, de nos jours, préfère-t-on représenter Eschyle plutôt que Euripide ? » Sa réponse synthétique est : Eschyle a enchaîné Prométhée. Cet enchaînement a en effet donné lieu, en Grèce, à un double débat.

Prométhée était-il un bienfaiteur ou un démon chargé de tarauder l'humanité ? Quel rôle pour Dieu/Zeus : accorder grâce à Prométhée ou assurer son châtiment ? L'étincelle de la raison, du progrès, et de la science son application majeure, avait en Grèce, il y a vingt-cinq siècles, ouvert un champ nouveau à l'humanité en changeant, en élargissant sa conception du monde. Ce moment fut hélas bref. Dès le siècle suivant, avec la fin tragique pour Athènes de la guerre du Péloponnèse, l'inquiétude prévaut au détriment de la curiosité, de l'éveil et de l'ambition.

On voit bien quel parallèle peut être fait avec notre époque où les interrogations débouchent souvent sur la décision de ne rien changer, de ne rien faire. C'est ainsi qu'a été malheureusement inscrit dans la Constitution française le principe de précaution. Nous aurions pourtant dû être prévenus de ses conséquences funestes. Une explication de la victoire de l'homme de Cro-Magnon sur Neandertal pourrait être en effet que notre ancêtre avait réussi à convaincre son cousin qu'il était dangereux de manier le feu, de tailler le silex, de tanner les peaux, d'inventer la roue et d'aller à la chasse sans précaution… Bref, il est temps de réagir. Renonçons tous ensemble au principe de précaution ! Modifions notre Constitution. Saisissons nos représentants et demandons-leur de rendre un peu de place à l'espérance, au bon sens et à la science, conclut avec force Thierry Derez.

Thierry Derez remet ensuite à Antoine Lefébure, au nom du jury, le **trophée d'or** du prix Risques 2015.

Antoine Lefébure, après avoir souligné son plaisir d'être ce soir à la Maison de l'assurance, prononce les quelques mots qui suivent :

« Avoir été sélectionné par la revue *Risques* pour recevoir ce prix m'a énormément touché et je vous remercie de m'honorer de cette distinction. Votre collège a, cette année, retenu mon livre, *L'affaire Snowden, comment les États-Unis espionnent le monde*. Un sujet qui pourrait sembler loin de vos préoccupations professionnelles mais qui, en fait, est au cœur de la problématique du risque.

Historien de formation, j'ai toujours manifesté un immense intérêt pour les usages des nouvelles technologies. Après une thèse sur le monopole des télécommunications en France, je suis passé à la pratique en lançant le mouvement des radios libres qui finira par l'emporter en 1981. Ce succès me propulse dans l'univers de l'entreprise. Le groupe Havas dont j'ai dirigé le développement avec comme dossier phare Canal Plus et ce qu'on appelait à l'époque « l'information automatisée ». Ce fut ensuite l'enthousiasme de participer au formidable essor d'Internet dès 1995, un peu trop tôt d'ailleurs, ce qui m'a obligé à faire autant de pédagogie que de business. Se voir confier la conception des sites Web de Virgin, de l'Ifop ou du premier Ministre, pour ne citer qu'eux, m'a immergé un peu plus dans les logiques subtiles entre l'information à délivrer et la technologie. Une nouvelle ère s'annonçait.

Dès que l'affaire Snowden a éclaté, j'ai immédiatement saisi les conséquences mondiales des informations dévoilées par ce lanceur d'alerte. Les enjeux d'une technologie au service de quelques individus sans contrôle n'allaient pas tarder à créer une onde de choc, et dans les institutions gouvernementales, et dans les grandes entreprises. Les dérives dans l'usage des technologies et les risques que cela soulève, voilà ce qui nous préoccupe aujourd'hui. L'activité sans contrôle de la NSA a piégé les logiciels, les appareils et les réseaux, faisant d'Internet le lieu de tous les dangers. Des logiciels espions et des virus destructeurs utilisés sans discernement pour des opérations légitimes se sont trouvés dans les mains d'organisations criminelles. La firme Symantec a annoncé qu'en 2013, 525 millions de personnes ont eu leur identité volée et que 25 000 Américains sont victimes chaque jour de vols d'informations médicales. Une multinationale comme Sony qui pensait avoir protégé correctement son système d'information s'est retrouvée victime d'un piratage qui a fait la une de la presse mondiale.

Rétablir la confiance sur les matériels et les logiciels, contrôler au niveau national et international la cybercriminalité deviennent des enjeux primordiaux.

Les révélations du jeune Edward Snowden m'ont conduit à une réflexion sur les redoutables transformations que les technologies du numérique génèrent. Nous voyons apparaître de nouveaux pouvoirs comme les associations délinquantes, avec pour conséquence un essor de la responsabilité et de l'activité des agences de renseignement.

Nouveaux risques, nouveaux conflits, il nous faut penser aux moyens à mettre en œuvre pour garantir notre sécurité collective tout en préservant notre vie privée et nos libertés individuelles.

Suite au retentissement qu'a provoqué la sortie de mon livre, j'ai été sollicité à plusieurs reprises par de hautes instances de la magistrature, par le Sénat, par les avocats ; j'ai pu affiner mes réflexions grâce à un débat aussi fructueux que passionnant. Pour résumer, on observe deux types de surveillance :

- la surveillance globale que tous les parlements européens s'accordent à considérer comme attentatoire aux libertés et inefficace dans la lutte contre la délinquance ;

- et la surveillance ciblée, celle qui doit concentrer tous les efforts parce qu'elle concerne des individus identifiés, repérés comme individus à risques et envers lesquels on dimensionne les investigations.

Aujourd'hui, l'heure est au réarmement moral face aux ennemis de la liberté qui voudraient nous tétaniser par la peur. Le superbe mouvement qui a vu en France cinq millions de personnes descendre dans la rue, en bravant leur appréhension, prouve la force des ressorts qui animent les Français. Cela fait écho à ce que disait Franklin Roosevelt en 1933 : « La seule chose dont nous devons avoir peur, c'est la peur elle-même ».

Depuis Hobbes et Locke, un consensus s'est mis en place pour reconnaître à l'État le rôle de puissance commune, seule capable d'assurer avec sécurité la gestion des contradictions entre les intérêts particuliers et l'intérêt général.

Face à la déstabilisation généralisée produite par l'essor fulgurant d'Internet, il nous faut élaborer un nouveau contrat social qui fasse prévaloir la sauvegarde des grands principes qui fondent notre vivre ensemble. Cette problématique n'est pas nouvelle. En 1932, le philosophe Carl Schmitt s'interrogeait : « Quelle politique sera assez forte pour assujettir la technique moderne ? »

Cet équilibre d'une gestion intelligente des risques et des opportunités nous permettra de sauvegarder notre existence d'individu désirant et agissant. Souvenons-nous de ce qu'écrivait Thomas Hobbes dans son célèbre ouvrage, *Le Léviathan* : « L'objet du désir d'un humain n'est pas de jouir une fois seulement et pendant un instant, mais de ménager pour toujours la voie de son désir futur. »

Comment rendre compatible le nécessaire renforcement des moyens de renseignement et de police avec la protection de nos libertés fondamentales ? La mauvaise gestion par les institutions américaines de la situation est très instructive, les excès du Patriot Act et de la NSA en témoignent.

Notre vieux pays est en mesure d'éviter ces errements en désacralisant le secret d'État et en établissant un tiers de confiance, une autorité de contrôle qui assurerait un suivi a priori et a posteriori des actions montées entre les services de renseignement et l'exécutif. Juges, parlementaires, personnalités qualifiées, cocktail d'arbitres indépendants et assermentés au service de la sécurité des citoyens.

Je fais confiance aux forces vives qui existent dans mon pays, un pays qui pourrait encore impressionner le monde, et j'ai confiance en l'humanité pour relever ce qui est sans doute l'un des grands défis des années à venir » conclut Antoine Lefébure.

Thierry Derez remet ensuite le **trophée d'argent** à Gérald Bronner.

Après avoir remercié le jury, ***Gérald Bronner*** s'est tout d'abord réjoui en quelques mots d'avoir pu

constater, à l'écoute des précédentes interventions, que ses préoccupations d'universitaire étaient beaucoup plus largement partagées que le débat public pouvait le lui laisser craindre. Il partage en effet à la fois les inquiétudes et les espoirs qui ont été exprimés. Ses inquiétudes s'illustrent par exemple par ce que l'on entend ces derniers jours sur la « théorie du complot » autour des récents et dramatiques attentats. La dérégulation du marché de l'information est en effet propice à la diffusion d'idées curieuses, à une démagogie cognitive permanente qui envahit l'espace public. La perception du risque ne fait pas exception à la règle, ne serait-ce que par ce que notre cerveau est mal équipé pour penser raisonnablement le risque : nous exagérons intuitivement les très faibles probabilités par un facteur dix ou quinze, nous mesurons mal les rapports coût/bénéfice, nous surestimons le coût de l'action par rapport à celui de l'inaction, etc. Tout cela trouve sa traduction dans le principe de précaution, figure de l'idéologie anti-prométhéenne qui s'est développée au cours du XX^{e} siècle. *Réenchanter le risque*, pour prendre le parti pris de l'espoir, ne doit donc pas être un vœu pieu. C'est une absolue nécessité pour notre destin collectif, pour le destin de l'Europe et pour celui de la France. Ceux qui seront incapables de prendre des risques se condamnent à rester en marge de l'histoire. Il n'est pas de plus grand risque que de ne pas en prendre, conclut Gérald Bronner.

Jean-Hervé Lorenzi remercie à nouveau les acteurs de cette soirée studieuse et amicale, la FFSA pour son accueil, le jury présidé par Daniel Zajdenweber et le Comité éditorial de la revue, les 101 contributeurs au numéro 100 et tout particulièrement ceux qui sont présents ce soir, les deux lauréats enfin du prix Risques. Lisons sans prendre de précaution leurs ouvrages et le numéro 100 de Risques !

VENTE AU NUMÉRO - BULLETIN D'ABONNEMENT

		Prix France
1	Les horizons du risque.	ÉPUISÉ
2	Les visages de l'assuré (Ière partie).	19,00
3	Les visages de l'assuré (2e partie).	19,00
4	La prévention.	ÉPUISÉ
5	Age et assurance.	ÉPUISÉ
6	Le risque thérapeutique.	19,00
7	Assurance crédit/Assurance vie.	19,00
8	L'heure de l'Europe.	ÉPUISÉ
9	La réassurance.	ÉPUISÉ
10	Assurance, droit, responsabilité.	ÉPUISÉ
11	Environnement : le temps de la précaution.	23,00
12	Assurances obligatoires : fin de l'exception française ?	ÉPUISÉ
13	Risk managers-assureurs : nouvelle donne ?	23,00
14	Innovation, assurance, responsabilité.	23,00
15	La vie assurée.	23,00
16	Fraude ou risque moral ?	23,00
17	Dictionnaire de l'économie de l'assurance.	ÉPUISÉ
18	Éthique et assurance.	23,00
19	Finance et assurance vie.	23,00
20	Les risques de la nature.	23,00
21	Assurance et maladie.	29,00
22	L'assurance dans le monde (Ire partie).	29,00
23	L'assurance dans le monde (2e partie).	29,00
24	La distribution de l'assurance en France.	29,00
25	Histoire récente de l'assurance en France.	29,00
26	Longévité et dépendance.	29,00
27	L'assureur et l'impôt.	29,00
28	Gestion financière du risque.	29,00
29	Assurance sans assurance.	29,00
30	La frontière public/privé.	29,00
31	Assurance et sociétés industrielles.	29,00
32	La société du risque.	29,00
33	Conjoncture de l'assurance. Risque santé.	29,00
34	Le risque catastrophique.	29,00
35	L'expertise aujourd'hui.	29,00
36	Rente. Risques pays. Risques environnemental.	ÉPUISÉ
37	Sortir de la crise financière. Risque de l'an 2000. Les concentrations dans l'assurance.	29,00
38	Le risque urbain. Révolution de l'information médicale. Assurer les OGM.	29,00
39	Santé. Internet. Perception du risque.	ÉPUISÉ
40	XXIe siècle : le siècle de l'assurance. Nouveaux métiers, nouvelles compétences. Nouveaux risques, nouvelles responsabilités.	29,00
41	L'Europe. La confidentialité. Assurance : la fin du cycle ?	29,00
42	L'image de l'entreprise. Le risque de taux. Les catastrophes naturelles.	29,00
43	Le nouveau partage des risques dans l'entreprise. Solvabilité des sociétés d'assurances. La judiciarisation de la société française.	29,00
44	Science et connaissance des risques. Y a-t-il un nouveau risk management ? L'insécurité routière.	29,00
45	Risques économiques des pays émergents. Le fichier clients. Segmentation, assurance, et solidarité.	29,00
46	Les nouveaux risques de l'entreprise. Les risques de la gouvernance. L'entreprise confrontée aux nouvelles incertitudes.	29,00
47	Changements climatiques. La dépendance. Risque et démocratie.	30,50
48	L'impact du 11 septembre 2001. Une ère nouvelle pour l'assurance ? Un nouvel univers de risques.	30,50
49	La protection sociale en questions. Réformer l'assurance santé. Les perspectives de la théorie du risque.	30,50
50	Risque et développement. Le marketing de l'assurance. Effet de serre : quels risques économiques ?	ÉPUISÉ
51	La finance face à la perte de confiance. La criminalité. Organiser la mondialisation.	30,50
52	L'évolution de l'assurance vie. La responsabilité civile. Les normes comptables.	ÉPUISÉ
53	L'état du monde de l'assurance. Juridique. Économie.	31,50
54	Industrie : nouveaux risques ? La solvabilité des sociétés d'assurances. L'assurabilité.	31,50
55	Risque systémique et économie mondiale. La cartographie des risques. Quelles solutions vis-à-vis de la dépendance ?	31,50
56	Situation et perspectives. Le gouvernement d'entreprise : a-t-on progressé ? L'impact de la sécurité routière.	31,50
57	L'assurance sortie de crise. Le défi de la responsabilité médicale. Le principe de précaution.	31,50
58	La mondialisation et la société du risque. Peut-on réformer l'assurance santé ? Les normes comptables au service de l'information financières.	31,50
59	Risques et cohésion sociale. L'immobilier. Risques géopolitiques et assurance.	31,50
60	FM Global. Private equitry. Les spécificités de l'assurance aux USA.	31,50
61	Bancassurance. Les agences de notation financière. L'Europe de l'assurance.	33,00
62	La lutte contre le cancer. La réassurance. Risques santé.	33,00
63	Un grand groupe est né. La vente des produits d'assurance. Une contribution au développement.	33,00
64	Environnement. L'assurance en Asie. Partenariats public/privé.	ÉPUISÉ
65	Stimuler l'innovation. Opinion publique. Financement de l'économie.	ÉPUISÉ
66	Peut-on arbitrer entre travail et santé ? Réforme Solvabilité II. Pandémies.	ÉPUISÉ
67	L'appréhension du risque. Actuariat. La pensée du risque.	ÉPUISÉ
68	Le risque, c'est la vie. L'assurabilité des professions à risques. L'équité dans la répartition du dommage corporel.	ÉPUISÉ
69	Gouvernance et développement des mutuelles. Questionnement sur les risques climatiques. La fondation du risque.	ÉPUISÉ
70	Ière maison commune de l'assurance. Distribution dans la chaîne de valeur. L'assurance en ébullition ?	35,00
71	Risque et neurosciences. Flexibilité et emploi. Développement africain.	35,00
72	Nouvelle menace ? Dépendance. Principe de précaution ?	35,00
73-74	Crise financière : analyse et propositions.	65,00
75	Populations et risques. Choc démographique. Délocalisation.	35,00
76	Evénements extrêmes. Bancassurance et crise.	35,00
77	Etre assureur aujourd'hui. Assurance « multicanal ». Vulnérabilité : assurance et solidarité.	36,00
78	Dépendance... perte d'autonomie analyses et propositions.	36,00
79	Trois grands groupes mutualistes. Le devoir de conseil. Avenir de l'assurance vie ?	36,00
80	L'assurance et la crise. La réassurance ? Mouvement de prix.	36,00
81-82	L'assurance dans le monde de demain. Les 20 débats sur le risque.	65,00
83	Le conseil d'orientation des retraites. Assurance auto, la fin d'une époque. Y a-t-il un risque de taux d'interêt ?	36,00
84	Gras Savoye, une success story. L'assurance, objet de communication. L'assurance, réductrice de l'insécurité ?	36,00
85	Solvabilité II. L'aversion au risque.	36,00
86	Un monde en risque. Le risque nucléaire. Longévité et viellissement.	37,00
87	Segmentation et non discrimination. Vieillissement : quels scénarios pour la France ?	37,00
88	Sport, performances, risques. Des risques pays aux dettes souveraines.	37,00
89	Le risque opérationnel, retour au réel. Vieillissement et croissance.	38,00
90	Les risques artistiques, industriels et financiers du cinéma. Les institutions et opérateurs de la gestion des risques au cinéma.	38,00
91	Les tempêtes en Europe, un risque en expansion. L'actif sans risque, mythe ou réalité ?	38,00
92	L'assurance vie : la fin d'un cycle ? L'assurance européenne dans la crise.	38,00
93	Protection sociale, innovation, croissance. Les ressources humaines dans l'assurance, préparer 2020.	39,00
94	Risque et immobilier. Mythes et réalités du risque de pandémie.	39,00
95	*Big data* et assurance. Les risques psychosociaux en entreprise.	39,00
96	Les risques dans l'agroalimentaire. Et si l'assurance était vraiment mondiale ?	39,00
97	Les nouveaux défis du risque transport. Le risque de réputation, le mal du siècle.	39,00
98	Quelle assurance pour les risques majeurs ? Les réseaux sociaux bouleversent l'assurance.	39,00
99	Le poids de la fiscalité sur l'assurance. Les gaz de schiste, une solution alternative ?	39,00
100	101 personnalités répondent à Risques	39,00

Numéros hors série : Assurer l'avenir des retraites - 15,24 • Crise financière : analyses et propositions 65,00 • Numéro spécial 20 ans : les 20 débats sur le risque 65,00

Où se procurer la revue ?

Vente au numéro par correspondance et abonnement

Seddita
26, boulevard Haussmann, 75009 Paris
Tél. 01 40 22 06 67 - Fax : 01 40 22 06 69
Courriel : info@seddita.com
www.seddita.com

Librairie partenaire

CNPP Entreprise Pôle Européen
de Sécurité - CNPP Vernon
BP 2265 - 27950 Saint-Marcel
Tél. 02 32 53 64 32 - Fax : 02 32 53 64 80

BON DE COMMANDE DE LA REVUE RISQUES

À découper et à retourner accompagné de votre règlement à

Seddita - 26, boulevard Haussmann, 75009 Paris

Tél. (33) 01 40 22 06 67 - Fax : (33) 01 40 22 06 69 - Courriel : info@seddita.com

❑ Abonnement annuel (4 numéros) FRANCE 142 € EXPORT 162 €*

❑ Je commande _____ ex. des numéros _____

Nom et prénom _____

Société : _____

Adresse de livraison _____

_____

Code postal _____ Ville _____

Nom du facturé et Adresse de facturation _____

_____

E.mail _____ Tél. _____

❑ Je joins le montant de : _____ par chèque bancaire à l'ordre de Seddita

❑ Je règle par virement en euros sur le compte HSBC 4 Septembre-code banque 30056-guichet 00750-07500221574-clé RIB 17

* Uniquement par virement bancaire