Risques

Risques

Les cahiers de l'assurance

N° 113

n° 113 - Trimestriel - Mars 2018

SEDDITA

Comité éditorial

Comité scientifique

Sommaire - n° 113 -

1. *Société* Prospérer dans le cybermonde

2. *Risques et solutions* Se protéger face aux cyberattaques

3. *Analyses et défis* Sécuriser et valoriser les parcours professionnels

4. *Études et débats*

Éditorial

En ce début de XXIe siècle, de manière discrète, quasiment imperceptible, apparaît un phénomène en réalité majeur, un glissement sémantique qui substitue progressivement au terme risque, celui de danger. Ce n'est pas le fruit du hasard, cela correspond à la réalité de la perception d'une grande partie de la population mondiale. Celle-ci, ne se sentant plus protégée, remet en cause tous les pouvoirs institutionnels, notamment le pouvoir politique, jugé bien impuissant face aux malheurs du monde. Pourquoi ce changement est-il si important ? Parce qu'en réalité cette utilisation désormais permanente du mot danger a une signification très simple ; oui le monde apparaît comme dangereux, en raison notamment des problèmes de sécurité, des tensions géo-stratégiques, de l'angoisse du retour des guerres ; mais ce phénomène touche également les marchés financiers, dont chacun attend la prochaine crise, considérée comme inévitable et surtout liée au développement de produits financiers incontrôlables. Alors bien sûr on régule, on réunit les organisations internationales, mais on a le sentiment que brutalement l'histoire humaine retrouve ses vieux démons et que cette relative période de calme et de coopération n'était que transitoire. Or, on ne peut rester avec un univers de simples perceptions qui désormais guideraient nos comportements. Et cela est d'autant plus dangereux que ces perceptions sont souvent – dans leur caractère excessif – le fruit de fantasmes et d'irrationalités. C'est donc l'objectif ambitieux que s'est proposé ce numéro de *Risques*, attaquer les domaines qui évoquent le plus la notion de danger et tenter de ramener leur gestion dans notre univers, celui de l'exigence et de la rationalité, celui de la théorie des risques. Pour cela, nous ne nous sommes pas effrayés des thèmes à traiter puisque nous avons débuté ce numéro par l'interview particulièrement stimulante du président de l'une des plus grandes sociétés mondiales de services informatiques, Paul Hermelin, qui nous a conduits dans les arcanes de la cybersécurité et les développements de la mondialisation, bien évidemment en Inde, son territoire de prédilection.

Ensuite, dans la rubrique « Risques et solutions » nous avons étudié l'univers terrorisant des cyberattaques, dont on ne voit qu'une infime partie des risques qu'elles comportent et des conséquences énormes qu'elles peuvent entraîner, et surtout dont on ne sait pas trop aujourd'hui comment les maîtriser. Inutile de dire que ceci représente sans nul doute un terrain de développement majeur pour l'assurance dans les années qui viennent. Dans la rubrique « Analyses et défis », nous nous sommes penchés sur ce qui est également perçu comme un grand danger dans nos sociétés contemporaines, à savoir les transformations profondes des marchés du travail. Car en fait, les parcours professionnels dans les années à venir seront l'un des problèmes les plus aigus que nos sociétés auront à régler. Pourquoi ? Tout simplement parce que le monde numérique segmente de manière cruelle et malheureusement très efficace, et les très qualifiés, et les autres, c'est-à-dire tous ceux qui, classes moyennes à qualifications moyennes, travailleurs non qualifiés, se voient réduits à des travaux d'exécution sans perspectives et sans possibilités de retour dans un univers plus favorable. Car c'est la caractéristique du marché du travail aujourd'hui, cette bipolarisation qui cantonne les uns et promeut les autres sans que le passage d'une catégorie à une autre ne soit ni aisé ni prévu ; c'est à cela qu'on attribue le vote dit populiste. Mais la liste des dangers est beaucoup plus importante. Nous avons également lancé un débat sur la sécurité routière qui demeure au cœur des angoisses des uns et des autres. Partout on le voit, nous sommes enclins à nous éloigner d'un regard scientifique sur tous ces thèmes. Ce numéro de *Risques* participe d'un retour à plus de rigueur.

Jean-Hervé Lorenzi

1.

Prospérer dans le cybermonde

Paul Hermelin

Président-directeur général, Capgemini

Paul Hermelin

Président-directeur général, Capgemini

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

Risques : Vous êtes à la tête de la première entreprise de services du numérique en France. Quels sont les risques auxquels vous êtes exposé ? Quelle perception en avez-vous ?

Paul Hermelin : L'informatique a toujours été un métier à risque ; un certain pourcentage de projets échoue ou dérive fortement. Au milieu des années 1990, nous avions publié le pourcentage de nos projets réalisés dans les temps et les budgets définis. Nous étions arrivés à un chiffre relativement satisfaisant de 93 % et nous espérions qu'en le publiant, nous entraînerions nos concurrents à publier leur propre chiffre. Nos concurrents n'ont pas suivi et ils se sont plutôt servis de ce chiffre pour tenter de nous discréditer auprès de nos clients ; nous avons donc arrêté. Mais cela montre que nous vivons dans une industrie risquée. Par exemple, j'ai en tête le cas d'un transporteur ferroviaire qui avait voulu appliquer au monde du chemin de fer le système de réservation du secteur aéronautique qu'il venait de racheter ; cela s'est révélé un échec. De même, plus récemment, pour le système de paie d'une administration française. Nous n'étions impliqués ni dans l'un ni dans l'autre de ces projets, mais nous avons connu des dérives comme d'autres. Pour couvrir les risques inhérents à notre métier, au-delà de notre expertise technologique et managériale, nous avons mis en place une captive d'assurance. Aujourd'hui, il existe une diversité des risques à prendre en compte, dont les risques systémiques. À noter également, l'attention nouvelle portée à la corruption avec la loi Sapin 2 qui oblige les entreprises à établir une cartographie des risques et à mener des actions de prévention dans ce domaine spécifique.

Risques : Une partie de ce numéro est consacrée à la protection des données face aux cyberattaques. Dans votre métier, comment gérez-vous ce risque ?

Paul Hermelin : Le risque a changé. Il y a quelques années, nous avions des attaques rampantes. Les hackers ne voulaient pas se faire repérer. Ils entraient donc silencieusement dans le système pour voler les données. Le séjour d'un intrus dans un système était de plus de dix mois ; l'intrus entrait dans le système d'information, ne connaissant pas la géographie de sa cible, il commençait par naviguer discrètement pour ne pas se faire repérer. La protection cyber consistait à détecter et à neutraliser les intrus. Aujourd'hui, les attaques ont pour but de paralyser les systèmes en échange d'une rançon. C'est un tout nouveau modèle d'attaque.

Risques : Peut-on qualifier cela de terrorisme ?

Paul Hermelin : Pas encore. Ces attaques font davantage partie du registre du crime organisé.

Risques : Dans le secteur de l'assurance, la révolution numérique pourrait potentiellement faire diminuer notre matière assurable (avec la voiture connectée par exemple) et parallèlement l'augmenter avec l'assurance des cyber-risques. Quelle est votre perception des risques à venir ?

Paul Hermelin : La notion de risque donne lieu à un travail informatique considérable. Le *big data* permet de qualifier les risques différemment et pourrait conduire, pour des populations intéressées, sauf contraintes légales, à rendre obsolète le principe même de la mutualisation qui sous-tend l'assurance. Aux États-Unis, des assureurs calculent les espérances de vie des individus et donnent les dates escomptées

de décès à leur courtier. Le courtier est devant un client dont l'opérateur lui dit : gérez vos contrats et vos produits en tenant compte du décès possible à telle date, et pour probablement tel type de maladie. Les concepts de libertés individuelles et de mutualisation sont renvoyés dos à dos. En France, tout le monde est assuré contre les catastrophes naturelles mais un jour, des assurés qui n'ont aucun risque d'inondation pourraient tout à fait refuser de payer une assurance pour les autres.

Et puis il y a l'intelligence artificielle (IA). Je vous donne un exemple d'IA au profit d'un assureur aux États-Unis sur les risques commerciaux pour des locaux professionnels. Par exemple, notre IA va chercher dans les réseaux sociaux tout ce que les clients d'un restaurateur disent, y compris sur Facebook, sur Trip Advisor, partout, afin de d'établir des recommandations d'ajustement de prix de contrats d'assurance à l'assureur. Toutes les données possibles sont collectées, et l'analyse en langage naturel des mots-clés qui reviennent le plus souvent sur les réseaux sociaux permet de valider si l'établissement est sous stress commercial ou opérationnel et donc financier, et si l'assureur devrait soit augmenter ses primes, ou bien se désengager de ce risque. C'est une IA au sens où elle calcule elle-même ses corrélations, et une fois qu'on l'a programmée, elle adapte les mots-clés en fonction de ce qu'elle trouve et établit les meilleures corrélations. Elle identifie les risques de manière logique et sans prendre en considération la politique de prix de l'assurance. Nous en sommes là. Dans le secteur de l'assurance, l'intelligence artificielle pourrait remettre en question la fonction de mutualisation historique de l'assurance. On peut tout à fait imaginer que des personnes aient intérêt à sortir du système d'assurance et disent : « Vu mon risque santé, je sors du régime général de sécurité sociale français, parce que je m'assurerais dans de meilleures conditions dans un système privé. »

Enfin, en matière de cybersécurité, il y a les risques systémiques. Ils affectent tous les systèmes de communication en temps réel : systèmes de transaction financière, de télécommunication... Le transfert des données à l'extérieur de l'entreprise, via le *cloud computing*, vers des opérateurs qui mutualisent des processus, comme la gestion de la paie, représente un certain risque. Certaines entreprises se demandent même s'il ne faudrait pas réinternaliser leurs données face aux risques potentiels ? Afin de répondre à ces craintes, Amazon ou Microsoft Azure ont déployé des protections sur le *cloud* public ; l'ordre de grandeur de leur investissement dans ce domaine – un milliard de dollars par mois – est supérieur à celui des budgets des plus grandes entreprises. Mais, comme c'est apparu récemment, les puces qui sont à l'intérieur même des systèmes informatiques ont été conçues à l'époque où les problématiques de sécurité étaient abordées différemment. On créait des barrières, des *firewalls*, pour empêcher d'entrer. On se préoccupait peu d'avoir une technologie sécurisée à l'intérieur du système. Or l'affaire Spectre (Intel) a montré qu'il y avait une faille dans les microprocesseurs qui ont été développés pour améliorer la performance. Et on sait désormais qu'on ne pourra pas empêcher toutes les attaques. L'étape suivante est donc la remédiation. C'est en quelque sorte une « course à l'armement ». Nous avons en face de nous des gouvernements, des organisations, militaires ou non, le crime organisé, des hackers libertariens (comme les Anonymous) qui ont une vision différente de la société par conviction politique. Par ailleurs, nous sommes confrontés au risque humain qui est une grosse source de défaillance. On va donc de plus en plus vers l'automatisation du système. Il faut également déployer des outils de détection, des outils d'analyse des comportements sur les réseaux, pour être en mesure de voir ce qui se passe très rapidement, et s'assurer que les données stratégiques sont, elles, absolument protégées. Une partie du système d'information doit être inaccessible, mais vous devez en limiter le périmètre le plus possible sous peine de ne pas arriver à la protéger du tout si ce dernier est trop grand, ou alors à des coûts exorbitants.

Risques : Existe-t-il des solutions qui permettraient de limiter cette inflation des coûts ?

Paul Hermelin : Je pense que les systèmes d'information vont devoir être ségrégués en fonction de la sensibilité des données. Il y a une sensibilité de

l'opinion publique à la valeur symbolique ou intime de certaines données (le numéro de sécurité sociale par exemple), qui n'ont pas nécessairement une valeur économique pour ceux qui construisent le système d'information.

Dans le domaine de l'assurance, l'assurance santé et la télémédecine sont directement concernées. L'intelligence artificielle est un bon premier niveau pour orienter les malades et faire face aux déserts médicaux. Mais cela veut dire aussi que les données des patients, les conclusions que pourraient en tirer les sociétés d'assurance sont stockées dans des dossiers médicaux. C'est par ce biais que l'opinion publique va comprendre l'ampleur du phénomène. Et il y aura une discussion sur les IA : doit-on remettre le premier niveau de santé entre les mains d'une intelligence artificielle ? Économiquement, c'est très probablement la seule solution par rapport aux enjeux de la formation des médecins.

C'est une question de société. Il faut que la société réfléchisse à ce qu'elle veut assurer, à ce qui fait partie d'un devoir collectif. Quand on n'avait pas une connaissance aussi précise des risques, il n'était pas question de remettre en cause le principe de mutualisation. Maintenant que l'on peut acquérir cette connaissance, cela pourrait être différent…

Risques : Vous envisagez la ségrégation des systèmes d'information pour protéger les entreprises des hackers. Mais n'y a-t-il aucun moyen efficace de contrer ces attaques ?

Paul Hermelin : Au même titre que les services de sécurité qui suivent les opérations de commerce illicite, nous patrouillons le Dark Web (1) à des fins de protection, pour vérifier qu'aucune des données traitées par Capgemini n'y circule et prévenir nos clients le cas échéant. Car les fuites de données résultent en général d'erreurs humaines courantes. Évidemment, certains vont sur le Dark Web avec l'intention d'utiliser les données trouvées pour commettre des escroqueries, à la carte d'identité par exemple ; pour autant, personne n'a jamais cherché à policer le Dark Web. En effet, il n'y a aucune possibilité de le fermer ; aussitôt un autre portail serait ouvert. Économiquement, les escroqueries liées au Dark Web coûtent très cher. Les gouvernements ont leur logique, le crime organisé en a une autre. Pour l'instant, le rapport bénéfice/coût pour le crime organisé est très élevé. Très peu d'escrocs sont pris, la logistique est simple et donc les bénéfices très importants.

Pour en revenir à votre question, la meilleure protection aujourd'hui c'est la volatilité : créer des systèmes de communication volatiles pour que les données ne laissent pas de trace trop longtemps. D'où les modèles à la manière de Snapchat, qui ne permettent pas de retrouver les informations dans la durée. La pègre l'a bien compris. Les traces, dans les systèmes volatiles, durent quelques heures, à peine. C'est du temps réel.

Risques : Certains assureurs, en assurance dommages, misent beaucoup sur la reconnaissance des images pour indemniser les assurés plus rapidement. Avez-vous le sentiment que nous allons vers des progrès rapides dans ce domaine ?

Paul Hermelin : La reconnaissance d'images n'est pas encore perfectionnée. Cela va prendre du temps, encore sept à dix ans de développement ; par comparaison, la reconnaissance vocale – en langage naturel – a progressé plus rapidement et atteindra son meilleur niveau dans trois à cinq ans. On arrive même maintenant à tracer des émotions.

Peut-on aujourd'hui identifier un sinistre avec les technologies de reconnaissance d'images ? Avec des photos du lieu au moment où le contrat d'assurance a été souscrit, on arrivera tout au plus à reconnaître que c'est le même lieu. Pour automatiser la reconnaissance, il faut que les photos soient d'une certaine qualité. Peut-on vous identifier par reconnaissance faciale, sur les technologies mobiles que nous avons aujourd'hui ? Non, pas encore.

Risques : Comprendre la dimension du sinistre, et faire en sorte que cela déclenche l'indemnisation. L'enjeu pour les assureurs est de dire : votre plafond est inondé sur deux mètres carrés, par conséquent

voilà l'indemnisation correspondante, en le comparant avec une base de données et avec d'autres images. Est-ce réalisable ?

Paul Hermelin : C'est faisable sur des peintures, sur des bâtiments ; pas encore sur des meubles, ou sur des voitures parce qu'il faudrait identifier ce qui se passe derrière la carrosserie pour évaluer les dommages réels. Ce n'est pas encore au point. Prenez l'exemple des sites sur lesquels, quand vous vous connectez, on vous demande d'identifier des photographies pour vérifier si vous êtes un humain ou un robot. Cela prouve que l'humain arrive à détecter des choses que la machine ne peut pas encore faire.

Nous faisons, pour les sociétés d'assurance, du *claim processing*, avec du RPA (Robotic Process Automation). Nous mettons en place d'importants programmes d'automatisation. Ce sont les procédures, le *workflow* que l'on automatise, plus que l'analyse du dommage lui-même.

Prenons l'exemple le plus connu : les gens ne comprennent pas encore que leur téléphone portable peut permettre d'analyser leur style de conduite via le gyroscope intégré. L'assureur pourrait très bien ajuster son prix au style de conduite de l'individu.

Risques : Les Anglais le font déjà. C'est le *pay-how-you-drive*.

Paul Hermelin : Il y a quelques années, Scott McNealy, président-directeur général de Sun Microsystems, m'a dit : « *Privacy is over* ». Sa théorie était que les hommes vivaient dans des villages dans un monde rural, où il y avait un contrôle social, avec le curé, le bailli, l'environnement. On n'était pas dans un monde d'anonymat. La révolution industrielle s'est traduite par des grandes villes et la création d'un anonymat urbain ; et l'informatique est en train de nous ramener dans le village ancien, en détruisant la notion d'anonymat.

C'est une situation intéressante et compliquée sur le plan juridique et réglementaire. Par les comportements sur les réseaux sociaux, la vie privée ne l'est plus. Pourtant elle est très protégée. Il y a quelques années, nous avons voulu faire une sorte de Google des CV et des compétences dans le groupe. Nous avons développé un système et demandé à nos collaborateurs de mettre leur CV sur cet outil. Dans de nombreux pays, ils ont refusé parce qu'il s'agissait d'informations privées… que vous trouvez aisément sur LinkedIn où ils les ont eux-mêmes rendues publiques.

Risques : Capgemini a accompagné la transformation de milliers d'entreprises qui se numérisent et changent leur modèle économique grâce à vous. Vous contribuez à optimiser les chaînes de production sur le plan des livraisons et des coûts. Pouvez-vous nous en dire quelques mots ?

Paul Hermelin : Aujourd'hui, la dépense en technologie d'information, hors directeur informatique, représente plus de 50 % des dépenses (plus de la moitié du marché n'est pas sous l'autorité du directeur informatique) ; le directeur du marketing, le directeur de la *supply chain*, achètent de l'informatique. La vraie définition du digital, c'est l'appropriation par des non-informaticiens des technologies informatiques pour améliorer le business. Mais ce qui est le plus important, ce que les Français n'ont pas encore bien perçu, c'est ce que représente le bouleversement apporté par Amazon dans la distribution, par exemple. Les individus ont changé de comportement. À une époque, on allait faire les courses avec plaisir le samedi après-midi. Aujourd'hui les consommateurs ont trouvé une alternative avec l'e-commerce et les grands dépôts. Le rôle du digital dans l'évolution de la grande distribution est gigantesque. La transformation digitale est une révolution, pas seulement pour le commerce et la distribution, mais pour l'ensemble des secteurs de l'économie : l'industrie, l'énergie, les services publics, la banque, l'assurance…

Risques : Pouvez-vous nous parler de votre stratégie en Inde, notamment en termes de risques ?

Paul Hermelin : L'Inde est une démocratie traversée de tensions religieuses, dans une position géostraté-

gique délicate – qui se traduit par quelques émeutes, des paralysies dues notamment aux discussions actuelles sur l'accès à l'eau –, avec comme voisin le Pakistan, plutôt instable, et un grand voisin, la Chine, avec lequel les relations sont variables. Le monde occidental a développé son intelligence informatique en Inde, Capgemini mais aussi Cisco, Facebook, Apple, Microsoft. Les volumes d'information que l'on peut y traiter est incomparable. Nous avons voulu créer des alternatives à l'Inde en créant des plateformes au Vietnam, aux Philippines, en Pologne, au Maroc, au Mali. Mais tout revient toujours en Inde, en raison des volumes. Pour vous donner un ordre de grandeur, Capgemini a 100 000 salariés en Inde et un taux d'attrition de plus de 20 %. Nous recrutons plus de 20 000 personnes, juste pour remplacer les départs, 30 000 personnes par an pour suivre notre rythme de croissance.

Risques : 20 000 départs ! Ce chiffre est impressionnant. Quel est le pourcentage de salariés très qualifiés ?

Paul Hermelin : La majorité des salariés ont un bac + 4. On estime qu'il y a 3,5 millions et demi de salariés dans l'informatique en Inde. Ils passent d'une entreprise à une autre pour obtenir des promotions. Mais l'automatisation mise en place par de nombreuses sociétés pourrait entraîner une diminution de ce chiffre.

Risques : Quelle politique mène une grande entreprise française comme la vôtre en matière de responsabilité sociétale ?

Paul Hermelin : Nous avons mis en place une politique de diversité pour lutter contre les discriminations ethniques, le handicap... L'un des sujets importants dans notre secteur est l'emploi des femmes. En France, 26 % de nos salariés sont des femmes alors qu'en Espagne elles représentent 40 % des effectifs. Cet écart est dû au système éducatif français qui est à revoir car il n'incite pas les filles à aller vers certains métiers considérés comme masculins. Nous y travaillons.

En matière d'environnement, nous avons mis en place des programmes destinés à réduire notre empreinte carbone. L'informatique, les serveurs, les voyages, etc., consomment de l'énergie. Nous avons également décidé de réorienter notre politique de sponsoring social, pour lutter contre la fracture numérique, ce que nous appelons positivement la *digital inclusion*. Capgemini étant un acteur de digitalisation, il nous a semblé évident d'accompagner la société vers cette transformation. En France, nous sommes l'un des principaux acteurs privés de la Grande École du numérique ; nous menons des travaux dans les quartiers, nous accompagnons la formation au digital de personnes ayant quitté l'école très tôt. Notre objectif est de réorienter 80 % de nos programmes vers la *digital inclusion* en deux ans. C'est un gros chantier.

Risques : Faites-vous des choses en matière de ruralité ?

Paul Hermelin : Nous ne nous occupons pas de l'équipement en réseaux câblés. Mais dans le cadre de mon activité de conseiller municipal, qui n'est pas liée à Capgemini, j'essaie de faire comprendre que nous ne sommes pas tous obligés d'aller dans une grande ville pour créer des espaces de coworking. C'est un sujet important. Hors région parisienne, 24 % des emplois sont dans les villes de plus de 200 000 habitants. Depuis 2004, 84 % des emplois créés dans le privé l'ont été dans les villes de plus de 200 000 habitants. Si vous êtes le père d'un jeune homme ou d'une jeune fille dans une ville de moins de 200 000 habitants, la seule chose à faire aujourd'hui pour lui garantir un avenir professionnel est de l'envoyer dans une grande ville.

Note

1. Ensemble de sites Internet se trouvant sur un réseau crypté et non référencés par les moteurs de recherche traditionnels. Le partage y étant anonyme, il est donc connu pour des échanges de fichiers ou l'achat d'objets plus ou moins illégaux (par exemple, cybercrime).

2.

Se protéger face aux cyberattaques

INTRODUCTION

Gilles Bénéplanc

La transformation numérique de la société, qui a débuté dans les années 1990, constitue une nouvelle révolution dans l'histoire de l'humanité. Elle touche tous les secteurs des sociétés développées ; son impact est de plus en plus manifeste et son rythme semble s'accélérer. À ce titre, cette révolution digitale transforme profondément l'univers des risques auxquels nous sommes exposés. Si le bug de l'an 2000 s'est finalement révélé un non-événement, les cyberattaques WannaCry ou Petya ont prouvé par leur ampleur et la nature des victimes touchées la réalité d'une menace très dangereuse. En conséquence, beaucoup s'interrogent sur la capacité de nos organisations à s'adapter pour tirer tout le parti de ces progrès technologiques en en maîtrisant les risques associés.

La complexité de ces nouveaux risques tient en particulier à leur caractère multiforme où s'entremêlent risques purement technologiques, multiplicité de l'usage des données et criminalité omniprésente parfois issue des États eux-mêmes.

C'est ce thème passionnant que nous avons choisi de traiter dans cette rubrique, en espérant contribuer à une meilleure prise de conscience des enjeux et des défis que nous devons relever collectivement.

L'article de ***Philippe Lemoine***, qui ouvre cette rubrique, s'intitule « La malédiction des données » par analogie à la malédiction de la rente des pays riches en matières premières. Ce risque menace nos sociétés modernes – dominées par les grandes plateformes Internet – qui, en se soumettant sans réserve à une nouvelle idéologie du *big data*, nieraient le rôle fondamental des personnes dans les transformations issues de la révolution digitale.

Les deux articles suivants explorent l'aspect géopolitique de la cybersécurité. ***Julien Nocetti*** analyse comment la cybercriminalité devient un élément fondamental des rapports de force entre les États. ***François-Xavier Albouy*** décrit le cas de l'Estonie, qui a pu bâtir une sécurité digitale ouverte et inclusive à la suite des cyberattaques qu'elle a subies en 2007.

Eric Filiol étudie les spécificités des risques que la révolution numérique a engendrés : risques techniques proprement dits, risques de l'environnement technologique, contexte politique. Selon lui, les caractéristiques actuelles de ces menaces ne permettent pas d'affirmer que ces risques deviendront maîtrisables – ou assurables –, même après une période d'adaptation.

Laure Zicry montre que pour les entreprises les données sont un patrimoine qu'il faut protéger au même titre que les biens physiques. Pour faire face au double défi de se protéger des attaques tout en partageant les données, de nombreux gestionnaires de risques ont choisi de transférer ces risques cyber au marché de l'assurance.

Pour ***Arnaud Tanguy***, une des dimensions essentielles de la cybersécurité des organisations est d'intégrer le facteur humain, et donc d'impliquer les collaborateurs. Pour cela, les pratiques de l'engagement des collaborateurs, de formation et de contrôle doivent évoluer pour qu'une nouvelle culture de la sécurité devienne le meilleur rempart pour l'entreprise.

Michael Nguyen clôt cette rubrique et pose la question fondamentale du difficile équilibre entre les moyens technologiques à mettre en œuvre pour protéger les données personnelles et les questions éthiques que ces solutions soulèvent, tout particulièrement le contrôle de l'humain par l'intelligence artificielle.

La malédiction des données

Philippe Lemoine

Président, Fondation Internet nouvelle génération (Fing)

Président, Forum d'action modernités

On dit parfois que les données sont le pétrole du XXIe siècle. La comparaison est hasardeuse mais elle a au moins ceci de juste que le pétrole est à l'origine de ce que les économistes ont appelé la malédiction de la rente et que nos économies pourraient bien connaître demain la malédiction des données. Que veut-on dire par malédiction de la rente ? C'est l'idée, vérifiée par plusieurs études empiriques, que les pays riches en matières premières, notamment en pétrole, et qui ont fondé leur développement sur cet avantage de la nature, ont connu des taux de croissance plus faibles que des pays équivalents mais privés de cet atout. Les raisons ? Un mélange de plusieurs effets : l'insécurité liée à la volatilité du cours des matières premières ; un effet taux de change qui fait que l'exportation de l'or noir enchérit la monnaie et nuit à la compétitivité-prix des industries naissantes ; et surtout cet effet rente qui fait que certains États pétroliers n'ont aucun besoin de lever l'impôt et ne jouent donc aucun rôle dans l'encouragement des nationaux à créer de la richesse. De même, parler de malédiction des données, c'est rappeler que la donnée n'est créatrice de valeur que combinée à d'autres facteurs et que vouloir s'en remettre isolément à elle est une dangereuse illusion. Pour prendre la mesure du danger, il n'est pas inutile de prendre d'abord un peu de recul et de suivre l'irrésistible ascension de la donnée qui nous a conduits à un certain vertige face au big data.

L'irrésistible ascension de la donnée

La donnée est un trou noir conceptuel. Personne ne sait définir clairement son statut. Cela lui donne une malléabilité qui en fait un attracteur puissant tout au long des grands cycles qui marquent l'histoire presque centenaire des technologies de l'information : 1936-1960, le cycle de l'ordinateur, depuis l'invention de son modèle théorique jusqu'à sa mise sur le marché ; 1960-1984, le cycle de l'informatique de gestion, des gros ordinateurs IBM jusqu'aux ordinateurs personnels ; 1984-2008, le cycle d'Internet et de l'informatisation de la société, avec le déploiement du réseau et l'informatisation des grands systèmes de transport, de santé, d'énergie, d'éducation ; depuis 2008, un nouveau cycle, celui de la transformation numérique de l'économie et de la société.

À l'origine, après la définition du concept de machine universelle par Alan Turing, la mise au point des ordinateurs va découler de l'idée qu'il faut rompre avec un modèle épistémo-technologique

selon lequel la prééminence du raisonnement, du programme, devait se traduire par une matérialité, par la fabrication de circuits logiques « en dur » qui traitaient un ensemble de données que l'on stockait depuis la mécanographie sur des cartes perforées. Le trait de génie de von Neumann fut de considérer que le programme était une donnée comme une autre et que l'architecture technique n'avait pas à les différencier. C'est de cette confusion qu'est né l'ordinateur.

Victorieuse, la donnée apparaissait dès lors comme dangereuse. Ne fallait-il pas se méfier de ce mélange de torchons et de serviettes ? Durant le cycle de l'informatique de gestion, le grand adage était « *garbage in, garbage out* » : si tu as des ordures en entrée, tu auras des ordures à la sortie. Une grande part de l'énergie investie dans la programmation était en fait consacrée à imaginer des contrôles : contrôles de présence, contrôles de cohérence, contrôles de vraisemblance. À l'heure des réseaux sociaux et des « *fake news* », il est étonnant que cette culture du contrôle paraisse s'être évaporée.

Le seul danger de la donnée n'est toutefois pas celui de l'erreur, de la donnée fausse. L'autre danger, c'est l'infobésité, l'excès de données insignifiantes, de données sans intérêt. Là encore, la donnée va fonctionner comme trou noir, comme catalyseur d'un nouveau progrès des technologies de l'information. L'étape suivante, celle d'Internet, provient en effet précisément du projet d'utiliser la puissance du réseau pour tarir à la source la prolifération des données sans valeur. Le Web naît à la fin des années 1980 au Centre européen de recherche nucléaire (Cern). Dans ce centre, ne se pose pas seulement un problème d'accès des chercheurs à la documentation scientifique, mais plus encore un problème d'excès d'informations, lié à ces gigantesques anneaux que sont les accélérateurs de particules, en particulier les collisionneurs. Dans ces immenses tunnels, des faisceaux contenant des milliards d'électrons et de positrons circulent à la vitesse de la lumière et entrent en collision 2000 fois par seconde. Chaque heure, les instruments enregistrent ainsi des milliards d'observations mais le taux de collisions utiles à la compréhension de la composition de la matière est extrêmement faible : au mieux, quelques-unes par an. Toutes les autres mesures n'ont aucun intérêt et le projet de Tim Berners-Lee et Robert Cailliau de créer un système hypertexte distribué sur le réseau informatique, trouve sa pleine justification dans la mise au point d'une architecture technique permettant d'écraser à la source les données inutiles.

Énergie noire, la donnée est toutefois extrêmement résiliente. Avec le passage à l'ère numérique, la donnée va rayonner plus que jamais. Pour tous les fabricants de tuyaux, de mémoires, d'ordinateurs, le *big data* est une bonne nouvelle. La chute des prix de transport, de stockage, de traitement est en effet impressionnante et cela aurait été une catastrophe si cette spirale déflationniste s'était combinée au succès d'approches sobres en données. Mais on revenait de loin ! Comment s'est déroulée cette dernière partie, celle qui débouche sur la représentation du gisement de données comme nouvelle source de richesse ?

Gloria, *big data* !

À l'âge numérique, le *big data* s'impose à la conjonction de trois champs de forces que l'on peut appeler les trois « V » : volume, valeur, vérité.

Volume : c'est la spectaculaire inflation du volume des données disponibles qui caractérise d'abord le *big data*. Selon IDC, la production annuelle mondiale de données croît à un rythme comparable à la célèbre loi de Moore : elle double tous les deux ans. D'ici 2020, sa taille globale devrait atteindre 44 zettaoctets, 10 puissance 21, 10 suivi de 21 zéros ! D'où vient cette explosion ? De l'accroissement des articles scientifiques ? Oui, mais pour une très faible part. Les gros volumes, ce sont les données de connexion, les mails et SMS, les traces de recherches, les commentaires sur les réseaux sociaux, les vidéos en tous genres, les mesures effectuées par les objets connectés... Les données structurées sous forme de fichiers de gestion ne représentent plus qu'une mince couche dans les

« *data lakes* » profonds qui s'imposent dans les grandes organisations comme extensions des anciennes banques de données. Tout un ensemble d'outils permettent de capter, de stocker, d'interroger, d'analyser ces gigantesques amoncellements de données.

Valeur : les grandes plateformes d'intermédiation électronique tirent une valeur boursière considérable de l'exploitation systématique des flux de données qu'elles captent méthodiquement. En juillet 2017, la capitalisation des Gafam s'élevait à 2 995 milliards de dollars : 785 pour Apple, 652 pour Google, 564 pour Microsoft, 500 pour Amazon, 494 pour Facebook. Cela représentait plus que le PIB de la France, 2 420 milliards de dollars. Pour toutes les entreprises de la planète, ce gonflement des valeurs boursières opère comme un marqueur de la voie à suivre. Il faut accumuler et exploiter le *big data* si l'on veut prospérer !

Vérité : au-delà d'une révolution technologique et économique, le *big data* se présente comme l'agent d'une révolution épistémologique, comme le catalyseur d'un nouveau régime de vérité. Les propositions commerciales s'affinent par la connaissance de la localisation des clients et par l'identification précoce de leurs préoccupations. La maintenance devient prédictive en analysant les vibrations, les usures, les gaz d'échappement. La police, la justice et la santé se veulent également prédictives. Les sciences sociales elles-mêmes fouillent ce qui s'échange sur les réseaux sociaux pour répondre à des questionnements sur les liens entre l'intime et le collectif et, à l'heure de la mondialisation, pour échapper aux limites nationales des grandes enquêtes statistiques.

Le bouleversement épistémologique ne s'arrête toutefois pas à cette exploitation humaine du *big data*. L'amoncellement de données est avant tout le socle à partir duquel progresse l'intelligence artificielle (IA). Le « *machine learning* », l'apprentissage automatique, est en effet la grande voie de développement de l'IA aujourd'hui, visant par l'entraînement des automates sur d'immenses jeux de données à les amener à reconnaître des formes et à sophistiquer des algorithmes de traitement. La qualité du *machine learning* est directement corrélée au volume du *big data* : nombre de cas, variété et qualité des attributs, pertinence des données renseignées. Il existe certes des exemples comme celui des jeux structurés par des règles (comme les échecs ou le jeu de go), où il a été récemment démontré que des réseaux neuronaux permettant à une machine d'apprendre en jouant contre elle-même un très grand nombre de parties, pouvaient être plus efficaces qu'un apprentissage à partir d'une base de parties réellement jouées par des humains (*cf.* AlphaGo Zero, octobre 2017). Mais, en règle générale, c'est le ratissage de données du réel qui alimente la structuration de l'intelligence artificielle.

La malédiction des données

Lorsque le *big data* cesse d'être pensé comme une simple ressource et devient une idéologie du salut, on s'approche de la malédiction des données. L'arbre « *data* » finit par cacher l'ampleur du tsunami numérique. La transformation numérique est en effet violente et trois aspects de cette violence risquent d'échapper à ceux qui s'en remettraient à l'illusion d'une richesse garantie par leur gisement de données.

La première violence à l'œuvre est celle du siphonage de la valeur qui s'opère au détriment des entreprises classiques et en faveur des grandes plateformes d'intermédiation. Dans le rapport sur la transformation numérique de l'économie française que j'avais remis en 2014 au gouvernement (1), j'évaluais la part de marché de la France dans la captation de valeur réalisée à l'échelle mondiale par les géants du numérique, à une ponction annuelle de 60 milliards d'euros prélevés sur les résultats de ses entreprises. Comment est-il possible d'y résister ? Pas seulement en s'équipant massivement de technologies ; des études ayant montré que les entreprises qui s'équipent, mais sans se transformer, ont des résultats qui s'effritent encore plus que ceux des entreprises qui ne font rien. Investir dans une politique massive de collecte, de stockage, d'analyse des données ? Cela ne saurait tenir lieu, à soi seul, de

stratégie de transformation. C'est le modèle même du grand groupe façon « *corporation* », issu de la seconde révolution industrielle, qui est mis à mal par la révolution numérique. La part de la politique y est trop importante, les coûts fixes des sièges sont sans utilité, l'innovation et l'initiative sont trop bridées à tous les niveaux. L'art, c'est de conjuguer les données avec un marketing clair des services, avec une conception renouvelée de la valeur ajoutée, avec un design intuitif, esthétique et limpide. C'est tellement éloigné de la culture de nombreuses grandes organisations, qu'elles sont condamnées à subir des stratégies de surtraitance de la part d'opérateurs numériques qui viennent s'interposer entre elles et leurs marchés, proposant aux personnes des formules souples et séduisantes d'agrégation de services et s'appuyant pour la livraison sur les acteurs existants, mais aux conditions de prix et de marge qu'ils ont définies.

La seconde violence que masque une certaine idéologie des données, c'est la négation de ce ressort nouveau à l'œuvre dans la révolution numérique : le rôle moteur joué par les personnes. C'est pourtant ce qui caractérise le cycle commencé en 2008, et ce n'est pas un hasard si l'on parle de *digital* en anglais et de numérique en français, deux mots qui viennent de l'électronique grand public. Ce sont en effet les personnes qui se sont équipées massivement de Smartphones et de tablettes qui font la course en tête. Au-delà de l'équipement, elles inventent les usages, défrichent de nouvelles façons de communiquer, d'échanger, de faire du troc, de produire, de partager. Les entreprises courent derrière pour capter ces innovations et imaginer des modèles d'affaires pour les rentabiliser. À l'image des acteurs les plus agiles du numérique, un élément clé de la transformation des entreprises traditionnelles devrait être d'apprendre à créer d'autres rapports avec les personnes, d'abolir les vieilles catégories figées de producteur ou de consommateur, d'apprendre les mécanismes de l'ouverture, de l'intelligence collective et de la coconception.

Au lieu de cela, l'idéologie data-centrique conduit vers l'impasse de vouloir redonner vie à une vieille lune : la patrimonialisation des données. Plutôt que d'acter le rôle moteur des personnes, on veut les voir comme des dominés qui seraient prêts à céder leurs données personnelles contre monnaie sonnante et trébuchante. On étend la logique du gisement de richesses et on laisse entendre aux personnes qu'elles seraient détentrices d'un trésor caché. Mais combien, les idéologues et les opportunistes qui prétendent cela, pensent-ils que le marché pourrait rémunérer ceux qui vendraient leurs données ? Hors de toute mise en perspective collective, hors de tout autre travail, les données ne valent rien ou pas grand-chose : quelques euros par an, quelques dizaines d'euros tout au plus. Les grands bénéficiaires de cette patrimonialisation seraient d'ailleurs les renards laissés libres de plumer, en toute légalité, le poulailler libre. Mieux vaut faire payer des impôts aux géants du numérique et promouvoir des instruments juridiques, comme le droit européen à la protection des données, qui défendent la liberté des personnes et instaurent une approche personnaliste du futur numérique !

La troisième violence que l'idéologie du *big data* a parfois tendance à voiler, c'est celle de la cybercriminalité publique et privée. Toutes les stratégies qui visent à amasser de grands volumes de données sont aujourd'hui menacées par le risque d'un hold-up informationnel. On sait qu'il en existe plusieurs types : vol massif, évaporation progressive, espionnage économique, virus, thromboses et chantage. Et, naturellement, on ne peut pas mettre vraiment dans le même sac les comportements des hackers privés, mafieux ou non, et ceux des hackers publics, dépendant ou non des services secrets. Mais les frontières sont parfois ténues... Depuis Snowden et les révélations sur les pratiques engendrées par le Patriot Act, on sait que les données sensibles sur les personnes détenues par les entreprises peuvent être détournées. Il n'y a pas de réponse technique absolue à ces risques. La meilleure réponse est celle de la vigilance de toute l'entreprise, à commencer par celle du patron. Mais l'expérience montre que les dirigeants préfèrent rêver aux perspectives heureuses du digital que de se confronter aux dures réalités de la cybersécurité.

La législation française n'étant pas a priori favorable à la constitution de mégabases de données polyvalentes,

nous n'avons pas connu en France de vols aussi massifs que ceux que connaissent les entreprises américaines. Pour des entreprises affaiblies par la difficulté de se transformer, ces scandales liés aux vols de données ont cependant un effet catastrophique. Ils viennent ruiner le capital confiance dont pouvait continuer de jouir une marque et finir de liquider ses forces.

Les monarchies pétrolières connaissent la malédiction de la rente. Dominées par les grandes plateformes, séparées des personnes par un matelas imaginaire de patrimoine numérique, soumises à la cybercriminalité publique et privée, les entreprises ou les nations qui voudraient s'en remettre au seul *big data* se condamneraient à la malédiction des données.

Note

1. Philippe Lemoine, « La nouvelle grammaire du succès. La transformation numérique de l'économie française », rapport au gouvernement, 2014. http://www.economie.gouv.fr/files/files/PDF/rapport_TNEF.pdf

La nouvelle géopolitique de l'Internet

Julien Nocetti

Chercheur, Institut français des relations internationales (Ifri)

Les événements internationaux de l'année écoulée ont replacé les problématiques numériques sur le devant de la scène diplomatique et stratégique. Les soupçons d'ingérence russe dans l'élection présidentielle américaine via les outils cyber et informationnel, les piratages massifs qui ont visé les sociétés Dyn et Yahoo, les rançongiciels de type WannaCry ou Petya et, plus globalement, la course aux cyberarmements, traduisent la volatilité d'une politique internationale bouleversée par la dissémination globale des moyens numériques.

Du numérique en politique internationale

Comment appréhender cette « géopolitique de l'Internet » qui se dessine sous nos yeux et ses enjeux, au-delà de la description d'une « cyberguerre » que l'on se plaît souvent à évoquer sans en maîtriser réellement tous les contours ? La question est posée avec une acuité nouvelle depuis les cinq dernières années tant pour les chancelleries, qui doivent adapter leur diplomatie, que pour les entreprises, principales cibles des cyber-attaques.

Tout d'abord, il faut bien comprendre la multiplicité des impacts de la transition numérique sur les politiques étrangères. Sur le plan stratégique, la transition numérique s'accompagne d'une rivalité entre puissances, en particulier entre les États-Unis et la Chine, et voit apparaître de nombreux acteurs non institutionnels pouvant disposer d'une influence globale (1).

Ces dernières années, l'industrie numérique américaine est devenue l'axe prioritaire tant du redéveloppement économique structuré autour de ces acteurs que de la stratégie de sécurité des États-Unis. Comme Ben Laden après le 11-Septembre, Edward Snowden contribue à refaçonner l'appareil de sécurité des États-Unis, redéployé autour de la surveillance électronique de la planète par la National Security Agency (NSA) et de « cyberopérations » qui se substituent aux coûteuses et risquées interventions extérieures. Internet participe aussi de la stratégie d'endiguement de la Chine et d'isolement de la Russie, grâce au contrôle des réseaux, à la définition des normes internationales, aux mesures protectionnistes contre les équipements chinois, à la captation des données et à la conclusion des accords commerciaux transatlantique et transpacifique, qui excluent ces deux pays. Le système institutionnel actuel permet aux États-Unis de conserver une influence juridique sans précédent, via la suprématie de leur droit souple et de la langue anglaise. Les débats sur la gouvernance de l'Internet sont, contrairement à l'Europe, suivis au plus haut niveau à Washington. Le statu quo savamment entretenu permet aux États-Unis d'éviter toute régulation internationale autre que technique de ce bien commun qu'est Internet (2). Plus globalement, les Gafam (Google, Amazon, Facebook, Apple et Microsoft) engendrent une forme nouvelle de pouvoir dont il est encore difficile d'esquisser les contours et les implications (3).

Sur le plan économique, le passage d'une économie de consommation de masse à une économie de la consommation personnalisée fait que certains pays – comme la France – souffrent d'un déclassement économique qui affaiblit leur puissance globale. La domination de l'économie numérique par les États-Unis et la Chine fait de la souveraineté numérique et de la maîtrise des données la condition sine qua non de l'autonomie stratégique. Ceci est encore plus vrai avec la convergence prochaine de l'économie des données, de la robotique, de la connectivité des objets et de l'intelligence artificielle. C'est ce que le Forum de Davos en 2016 avait appelé la « quatrième révolution technologique » et qui bouleverse non seulement la production mais aussi la vie des sociétés et l'équilibre du monde.

Sur le plan diplomatique, enfin, le numérique accélère la diffusion de la puissance à l'ensemble des acteurs sociaux. La diplomatie est maintenant diluée dans une gouvernance globale, des formes de régulation transnationale qui se multiplient et dans lesquelles les acteurs nationaux sont parfois écartés. Un grand nombre de normes internationales dans le champ numérique se sont ainsi mises en place sans passer par les canaux habituels de la diplomatie, ce qui rend celle-ci éminemment plus complexe.

Fin de l'innocence et diffusion de la menace

Il y a quelques années, la cybersécurité se limitait à quelques piratages de banques ou d'entreprises et ne parlait qu'à une poignée de spécialistes. Elle est, aujourd'hui, partagée par tous les citoyens. En d'autres termes, nos sociétés ont pris conscience de leurs vulnérabilités : l'ensemble de nos organisations et de nos nations est concerné.

Avant la présidence de Donald Trump, les États-Unis ont montré qu'ils pouvaient remettre en cause les piliers fondamentaux de la confiance de l'Internet à l'échelle mondiale, en sapant les soubassements des systèmes de sécurité utilisés partout sur la planète. Des programmes entiers de la NSA avaient pour objectif de créer des « portes dérobées » (*backdoors*) dans les systèmes de sécurité et d'affaiblir les systèmes de chiffrement. La vulnérabilité devient systémique et peut se retourner contre n'importe qui.

La cyberconflictualité se caractérise par la multiplicité des acteurs engagés. Les menaces peuvent venir d'États, d'organisations criminelles, mais aussi de simples pirates et sans doute, un jour, d'organisations terroristes. S'il est possible de négocier avec des États, cela est impossible avec des criminels ou des terroristes, ce qui rend inutile, par exemple, un traité de non-prolifération inspiré des pratiques établies depuis des décennies dans le domaine nucléaire. Elle se traduit également par une « extension du domaine de la lutte ». La nature des attaques est en effet très mouvante. Les États-Unis, Israël et la Russie semblent avoir déjà utilisé le cyber pour attaquer des infrastructures, et ces acteurs recourent, à des degrés divers, au cyberespionnage. La Russie, cependant, est soupçonnée d'avoir ouvert un champ de la « cyberguerre » : s'inviter dans le processus électoral d'un pays. En d'autres termes, on est passé de l'espionnage classique au sabotage politique. Pour certains États, comme la Russie mais aussi la Chine, l'objectif prioritaire d'une cyberattaque est de produire de l'incertitude politique – et idéalement de paralyser la prise de décision du pays visé. Le couplage entre cyberattaques et campagnes informationnelles ouvre ainsi de nouveaux champs en matière de cybersécurité, que les États comme les entreprises doivent appréhender de la manière la plus fine possible [4].

La responsabilité des États dans le cyberarmement

La question du contrôle des cyberarmes d'État est posée avec acuité depuis la révélation que le virus informatique WannaCry, qui a frappé plus de 250 000 ordinateurs lors d'un week-end de mai 2017, a été subtilisé à la NSA par des cybercriminels. Dans le monde entier, des hackers s'affairent pour débusquer des failles de sécurité de logiciels (*zero day*) pour le compte d'agences de renseignement. Ces arsenaux servent à pénétrer dans les systèmes informatiques de

leurs ennemis, qu'il s'agisse de gouvernements ou d'organisations terroristes.

En mars, WikiLeaks avait révélé que la CIA disposait de dizaines de failles pour pirater des iPhone et des smartphones Android, des ordinateurs équipés de Windows et même des téléviseurs Samsung. Cette course à l'armement, préoccupante, ne fait l'objet aujourd'hui que d'un contrôle minimal. Les Nations unies réfléchissent à des moyens supplémentaires de limiter la prolifération des cyberarmes, comme elles le font pour des armes conventionnelles – mais le droit international du cyberespace demeure à un stade embryonnaire. En février, Microsoft avait appelé à la signature d'une « convention de Genève du numérique », avec l'introduction de normes qui obligeraient les États à révéler aux éditeurs les failles de sécurité en leur possession.

Un nouveau cadre mondial doit aussi permettre de définir la manière dont un État ou ses entreprises ont le droit de riposter à une cyberattaque. Pour qu'il soit efficace, cet indispensable contrôle des cyberarmes suppose en parallèle de ne pas systématiquement chercher à affaiblir la sécurité des logiciels à des fins de surveillance. L'idée d'une riposte à une attaque par les entreprises peut sembler incongrue, mais les débats sont actuellement riches autour de ce que l'on appelle le *hack back*. Ce droit à détruire les données volées et à répliquer est défendu aux États-Unis et au Canada, et dernièrement par les services allemands (5). Il fait davantage débat en France – les autorités pointent les risques de surenchères résultant d'une telle démarche de « défense agressive » (6).

Attribuer ou pas ?

La cyberconflictualité ne vise pas uniquement le champ strictement politique. Elle cible de plus en plus les infrastructures dites critiques (énergie, télécommunications, défense). Ces dernières années, par exemple, les cyberattaques se sont multipliées dans le secteur de l'énergie. Le piratage des systèmes informatiques des monarchies pétrolières (Aramco), la mise hors service du réseau électrique ukrainien (piratage de la centrale d'Ivano-Frankivsk) et l'attaque contre les centrales nucléaires iraniennes en 2010 en constituent autant d'exemples. Les télécommunications et les médias subissent également de lourds dommages : TV5 Monde en 2015 et plusieurs plateformes et médias (New York Times, CNN, Financial Times, Twitter, etc.) à l'automne 2016.

Si la cybermenace se situe aux confins de l'espionnage économique, de la guerre politique et du crime organisé, les risques les plus sérieux proviennent d'États qui n'hésitent pas à mobiliser de larges capacités offensives à des fins de déstabilisation et de destruction, en s'abritant derrière l'incertitude de l'attribution. Il est encore très difficile d'identifier les auteurs d'une attaque, qui peuvent se cacher derrière une bande de hackers ou des ordinateurs installés dans un pays tiers (serveurs proxy). L'impossibilité de connaître son adversaire rend caduc le droit à la légitime défense et, par conséquent, empêche toute dissuasion comme dans le cas de la guerre nucléaire. L'attribution est un outil éminemment politique et fait évoluer les pratiques diplomatiques traditionnelles – on l'a bien vu avec les atermoiements de Barack Obama à l'automne 2016 lorsqu'il a été question d'attribuer ou non aux Russes les attaques et intrusions subies. Pour des raisons davantage d'ordre géostratégique, les Américains ne voulaient pas être les premiers à déclarer une cyberguerre. Une attaque américaine contre les réseaux russes, par exemple, ouvrirait une boîte de Pandore à la fois technique et juridique. Attribuer reste donc un acte politique seulement appuyé d'un faisceau d'indices.

L'Ukraine, théâtre d'une « cyberguerre » ?

L'Ukraine est massivement touchée depuis le déclenchement du conflit avec la Russie. Lors des premières révoltes de Maïdan à Kiev, en novembre 2013, un groupe de hackers prorusses, CyberBerkut, avait

piraté les serveurs de la Commission centrale électorale ukrainienne. Après l'annexion de la Crimée en mars 2014 et les premiers événements dans le Donbass, des attaques répétées contre des réseaux de télécommunications et des centrales électriques se produisirent dans le pays. S'ensuivit un véritable « pilonnage » des institutions, des acteurs économiques et de l'industrie ukrainiens (7).

Le 27 juin 2017, une puissante cyberattaque frappe l'Ukraine et, par effet boule de neige, se répercute dans nombre de pays, dont la France. Selon les experts, le ciblage sur l'Ukraine semble plutôt délibéré. Dans le cas de Petya/exPetr, les infrastructures critiques ont été affectées, pas uniquement les institutions : le système bancaire, les aéroports, les télécoms, l'énergie, les chemins de fer nationaux... Pas seulement un « patient zéro », l'Ukraine est la cible principale du logiciel malveillant dont l'objectif est de faire le maximum de dégâts. Il s'agit d'une attaque motivée non par l'appât du gain mais par le blocage pur et simple des réseaux d'entreprise : le blocage de données sans volonté de les rendre de nouveau accessibles peut constituer un motif suffisant pour déstabiliser un territoire et fragiliser l'État concerné (8).

L'ensemble de cette menace, diffuse et complexe, représente à l'évidence un défi suffisamment conséquent pour que les entreprises modifient leur approche de la cybersécurité. À l'argument, trop facilement invoqué, du fossé générationnel, il peut être rétorqué qu'il est nécessaire de se rendre compte du caractère stratégique des données au lieu de continuer à focaliser son attention sur les « technologies de l'information ». Ces défis seront accentués par la formidable explosion de l'Internet des objets. Selon les estimations, entre 20 et 50 milliards d'objets connectés existeront à l'horizon 2020… Ce qui laisse la porte ouverte à un niveau de vulnérabilité(s) tout à fait remarquable.

Notes

1. Voir le dossier « Internet : une gouvernance inachevée » dans la revue Politique étrangère*, n° 4, hiver 2014.*

2. Julien Nocetti et Françoise Massit-Folléa, « Internet se cherche une gouvernance », lemonde.fr*, 23 avril 2014.* http://www.lemonde.fr/idees/article/2014/04/23/internet-se-cherche-une-gouvernance_4405625_3232.html

3. En mars 2017, leur valorisation cumulée égalait presque le PIB de la France en 2016. Calculs réalisés par l'auteur.

4. Julien Nocetti, « Comment l'information recompose les relations internationales », in *Thierry de Montbrial et Dominique David (dir.),* Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, Dunod-Ifri, 2017, p. 141-142.*

5. Andrea Shalal, "German Spy Agencies Want Right to Destroy Stolen Data and 'Hack Back'", reuters.com*, 5 octobre 2017.* https://www.reuters.com/article/us-germany-cyber/german-spy-agencies-want-right-to-destroy-stolen-data-and-hack-back-idUSKBN1CA1IN

6. Émilie Laystary, « Faut-il autoriser le hack back*, entre légitime défense et escalade de la violence ? »,* mashable.france24.com*, 30 janvier 2018.* http://mashable.france24.com/tech-business/20180130-hack-back-legitime-defense-escalade-violence-entreprises-reverse-hacking

7. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", wired.com*, 20 juin 2017.* https://www.wired.com/story/russian-hackers-attack-ukraine

8. Amaelle Guiton, « Les cobayes de la cyberguerre », libération.fr*, 28 juillet 2017.* http://www.liberation.fr/futurs/2017/07/28/les-cobayes-de-la-cyberguerre_1586976

C'est une volonté politique qui a fait de l'Estonie la première société digitale

François-Xavier Albouy

Directeur de recherche, Chaire « Transitions démographiques, transitions économiques »

La société digitale n'est pas venue en Estonie de la puissance des magnats de l'high-tech et de riches commerçants en ligne, mais directement d'une volonté politique qui a bénéficié de circonstances historiques exceptionnelles. Il n'y a pas de défiance sociale vis-à-vis du numérique, mais au contraire la volonté de construire un projet de société ouverte qui s'incarne dans une inclusion numérique. C'est le politique qui a démarré, et ce au bénéfice des citoyens. Dans un pays en avance sur la transition démographique et sur l'égalité entre les sexes, cette révolution s'est accompagnée de plans ambitieux de formation pour les seniors et d'une politique salariale égalitaire entre les sexes. Ce sont aujourd'hui les entreprises et le secteur privé qui en bénéficient. La cybersécurité est un état d'esprit inscrit dans le système et le modèle insiste sur la résilience et la fiabilité.

Le digital, une réussite politique et sociale

Au moment où cet article est écrit, février 2018, plus de 30 000 personnes dans le monde ont pris une e-citoyenneté estonienne. Cette e-citoyenneté permet en quelques minutes, à tout le monde, de recevoir une carte d'identité qui authentifie toutes les transactions électroniques, et d'accéder à de nombreux services numériques. Elle ne permet pas d'avoir la nationalité estonienne, ni d'avoir sa résidence fiscale en Estonie. Son intérêt principal est de pouvoir monter immédiatement une entreprise, d'obtenir un compte bancaire et de commencer des transactions en ligne. Elle permet également de gérer cette entreprise depuis n'importe quel endroit dans le monde, et surtout d'accéder à des services sécurisés de transmission de données.

La carte ne coûte que cent euros et permet, par exemple, à un entrepreneur français n'ayant d'activités qu'en France de lancer son activité tout en bénéficiant de nombreux services et supports dématérialisés. À ce jour, 1 500 Français ont demandé la carte, ce qui place la France dans la moyenne des pays européens. Trouvant le concept séduisant, beaucoup demandent la carte mais la moitié créent réellement des entreprises. La plupart sont des entreprises individuelles de conseils et de développement informatique, mais tous les secteurs sont représentés. Très peu d'assureurs

ont franchi le pas : trois agents ou courtiers et un réassureur.

Il est permis de penser que ce développement va être exponentiel, et qu'au-delà de l'effet de mode, c'est depuis l'Estonie que de très nombreuses entreprises ou start-up vont conquérir le monde. La société digitale estonienne s'ouvre aux infrastructures privées et met à la disposition de tous l'une des technologies digitales les plus sécurisées de la planète. La sécurité n'est pas un frein à la digitalisation, mais une raison de son accomplissement.

L'Estonie n'est pas en avance sur l'économie digitale, elle est dans un autre temps, un au-delà de ce que nous connaissons. C'est en fait la seule réponse politique cohérente au déferlement de la vague digitale. Le gouvernement estonien a décidé en 1997 de basculer dans l'e-gouvernement, puis de prélever les impôts de manière digitale pour en 2001 développer le X-Road, architecture de gestion de bases de données sécurisées. Ces développements – qui aujourd'hui paraissent banals – étaient futuristes il y a vingt ans.

La réussite de ces développements n'est pas seulement technique, elle est d'abord politique et sociale. La société estonienne a dans son ensemble accepté cette mutation fondamentale, parce qu'elle a eu confiance. En France, comme dans les autres pays européens, les citoyens ont, en pratique, tendance à faire plus confiance à Google, Facebook et autres fournisseurs de services qu'à leur administration, leur employeur, pour ne pas parler de leur assureur...

La parcimonie à diffuser volontairement des données, parce qu'elles mettent en cause la vie privée, contraste avec le peu d'attention accordée par la diffusion implicite de données très personnelles sur les réseaux. 23 % des Européens ont déjà acheté quelque chose sur le Net – c'est remarquablement bas – et pourtant la plupart des Européens ont des comptes sur les réseaux sociaux qui permettent en théorie de tout connaître de leur vie privée, de leur patrimoine, de leur état de santé.

Une cybersécurité assumée et maîtrisée

Cette mutation vient d'une histoire récente et singulière. Lorsque l'URSS se décompose, les pays baltes choisissent tout de suite et très vite des modèles d'économie ouverte résolument tournés vers l'Europe de l'Ouest et les États-Unis, et une transformation rapide des structures économiques étatiques vers la privatisation. L'Estonie s'engage avec plus de force que ses voisins baltes dans cette voie. Sa proximité culturelle et linguistique avec la Finlande est un appui. Il s'ensuit un afflux considérable d'investissements étrangers, jusqu'à 40 % du PIB, loin devant ses voisins baltes qui stagnent autour de 10 à 20 %. La politique prudente évite un endettement excessif et la monnaie est rapidement stabilisée après une phase d'hyperinflation. L'État se construit sur une indépendance farouche vis-à-vis de la Russie, laquelle entraîne une hostilité latente, parfois explicite. La décision de ce petit pays de s'ancrer dans la modernité est encouragée par ce consensus politique, qui du centre droit au centre gauche, favorise une politique libérale et accepte une protection sociale plus réduite en contrepartie d'un chômage qui se résorbe rapidement. L'accent est mis sur le système éducatif, pour permettre la promotion politique de la langue estonienne. La participation des femmes au marché du travail est aussi l'une des plus élevées d'Europe et la différence de salaires entre les sexes, l'une des plus faibles. Bref, une mutation rapide, vers un pays ouvert et qui très vite adhère à l'Europe. La confiance dans le nouvel État démocratique est une donnée, la confiance dans l'État électronique sera du même ordre.

Lorsque les virus informatiques attaquent l'Estonie en 2007, dans une opération restée obscure mais largement attribuée aux services russes, tous les portails publics et la plupart des portails privés sont bloqués, certains quelques heures, d'autres quelques jours. Le monde découvre la réalité militaire de la cyberguerre. L'Estonie devient le leader en matière de

sécurité et c'est sur son sol que se crée une agence internationale de cybersécurité portée par l'Otan. Les Estoniens sont alors très attachés à leur mode de vie digitalisé, et loin de reculer ils approfondissent encore la digitalisation de la société, tout en développant une cybersécurité qui aujourd'hui fait école et dont s'inspirent tous les pays. Ces opérations de sécurité sont là aussi techniques – bases de données distribuées, données cryptées, localisation des données sur des sites multiples –, mais aussi et surtout sociales – création d'une unité de défense spécialisée au sein de l'armée, des entreprises, création d'un corps de volontaires dédiés à la cybersécurité.

Certes de nombreuses attaques malveillantes et de piraterie sont conduites en Estonie, comme partout dans le monde, mais la confiance ne se dément pas : l'idée est que la digitalisation comporte des risques et qu'il est possible de les atténuer. Les cyberattaques sont quotidiennes. On en a dénombré plus de 700 en 2017, qui ont coûté en Europe près de 750 milliards d'euros ou 5 % du PIB. Un système global peut-il être fiable ? La réponse est positive, l'Estonie n'a subi aucun dommage.

Cette confiance produit des effets impensables dans un pays comme la France, où l'essentiel du débat ne porte pas sur les intentions malveillantes, mais sur la protection de la vie privée. La sécurité est un état d'esprit, nous disent les Estoniens. Le problème n'est pas de sécuriser des données pour ne pas les utiliser, il est de pouvoir utiliser des données de manière sécurisée.

Deux décisions récentes témoignent de cette confiance et de l'accent mis sur la sécurité. La première est la décision d'ouvrir une ambassade électronique au Luxembourg, c'est-à-dire un lieu où sont stockées les données vitales du pays et de ses citoyens, un site miroir qui bénéficie d'une extra-territorialité pleine et entière, comme une représentation diplomatique et qui vise essentiellement à augmenter la résilience du système en cas de panne ou d'attaque. Imagine-t-on les politiques français prôner une duplication des données de santé des citoyens en Nouvelle-Zélande, par exemple, un autre des cinq pays les plus avancés dans la digitalisation ? Une deuxième réalisation récente est celle d'un vaste programme d'échanges de données développé avec la Finlande. Ce programme est impressionnant puisqu'il permet aux deux États de n'en faire plus qu'un au sens numérique. Il n'y a pas d'intégration politique ni de gouvernance commune mais les données sont partagées, ce qui simplifie singulièrement la vie des migrants entre les deux pays, la création d'entreprises communes, et accessoirement le travail du fisc !

Après une digitalisation à marche forcée depuis vingt ans, les réalisations sont étonnantes : pour les citoyens, tous les actes administratifs publics et privés sont numérisés, la carte d'identité virtuelle, les paiements, les droits sociaux, les dossiers scolaires, tout est numérique. Les données sont accessibles aux citoyens qui peuvent les modifier facilement. Tous les contrats sont numériques, l'infrastructure de l'État est ouverte aux entreprises, et les données bancaires, les contrats d'assurance, les contrats de travail entre les entreprises et leurs employés ou les contrats de prestations de services sont également numériques. Cela permet des rapports entre les citoyens et les autorités administratives publiques et privées plus fluides. Créer une entreprise en ligne se fait en quinze minutes et elle peut aussitôt commencer à travailler. Pour un citoyen, contracter en ligne avec une entreprise n'est pas une option, c'est la règle.

Toutes ces bases de données sont reliées par une infrastructure qui permet de crypter les données et de les échanger très simplement entre opérateurs.

Ce modèle de fluidité numérique, l'Estonie s'en fait le chantre et développe une politique résolue de coopération internationale très ouverte avec notamment la Namibie, la Biélorussie, l'Ukraine, le Kazakhstan, Singapour, la Nouvelle-Zélande et bien d'autres encore… Si la politique reste très défensive vis-à-vis de la Russie, force est aussi de constater que les citoyens russes sont les plus nombreux et actifs dans l'e-citoyenneté estonienne.

Pour quel avenir ?

Ce chantier prométhéen est fructueux, et tout le monde s'accorde sur des économies globales dans les frais de transaction d'environ 2 % du PIB, ce qui représente l'équivalent de cinq jours de travail. Quelle sera la prochaine étape ? Faire bénéficier pleinement les entreprises et le secteur privé de ces innovations. C'est déjà le cas en matière de santé avec la création d'une base de données génétiques de plus de 500 000 citoyens, base qui servira à développer de nouveaux traitements et médicaments. C'est aussi le cas dans les développements informatiques où des coûts administratifs très légers et un environnement favorable aux entreprises incitent le pays à aller encore plus loin. L'initiative gouvernementale Start-up Estonia offre de nombreux services : formation aux moyens de paiements, formation des investisseurs à l'évolution rapide des barrières réglementaires... L'ambition est considérable puisqu'il s'agit de lancer avec succès 2 000 start-up d'ici à 2020. Les projets sont à la hauteur de Skype, entreprise estonienne qui a révolutionné le monde des télécommunications. Une start-up envisage de créer une plateforme mobile de logistique pour des transports de marchandises maritimes disruptifs accessibles aux PME, partout dans le monde. Une autre invente un système équivalent pour le transport routier. Une troisième révolutionne le transfert d'argent. Une quatrième permet de créer en quelques clics son site Web, et ce, en répondant simplement par oui ou par non à un jeu de questions... Les exemples sont infinis et l'Estonie est en passe de devenir la Silicon Valley européenne. La Banque mondiale considère que l'Estonie est le pays le plus avancé dans ce qu'il est convenu d'appeler une société digitale. Bref, l'avenir est peut-être moins à San Francisco ou au sommet de Las Vegas, qu'il n'est dans les nombreux *workshops* de Tallin.

Les aspects exceptionnels et très séduisants du modèle estonien sont, d'une part, son ancrage politique marqué par le désir d'être un modèle en Europe, d'autre part, sa volonté d'inclure les seniors dans la transformation dans un pays vieillissant, et enfin son désir de coopération et d'ouverture.

Les premiers à en profiter sont les citoyens, qui ont tout de suite vu les bénéfices de relations simplifiées avec l'État ; un contraste majeur après la société soviétique. Dans le même ordre d'idées, l'instauration d'une société ouverte et digitalisée a probablement évité beaucoup des travers des autres sociétés de la transition en termes de domination des mafias et de la corruption. Un peu comme si l'Estonie avait décidé que le plus court chemin vers la social-démocratie à la scandinave passait par la digitalisation. On mesure aujourd'hui ce qui a pu provoquer des tensions avec la Russie. Après tout, le pays a accédé à l'indépendance sans prendre sa part de la dette soviétique avec une population peu nombreuse, homogène, très bien éduquée, et qui s'est reconstruit une histoire neuve. Cela explique certainement l'attaque cybernétique du 9 mai 2007, au moment où Moscou commémorait la fin de la grande guerre patriotique – laquelle est fêtée à Moscou le 9 mai et non le 8 mai pour des raisons de décalage horaire. Une statue déboulonnée qui, pour les uns symbolisait le sacrifice des Russes pour la libération de l'Europe et pour les autres, l'oppression soviétique, a avivé les tensions et est probablement la cause événementielle de l'attaque de 2007. Le Kremlin n'a jamais reconnu sa responsabilité dans cette attaque et tout juste concédé qu'elle venait d'un assistant parlementaire de la Douma et de hackers ultra-patriotes de Transnistrie. L'Otan a toujours maintenu qu'une attaque de cette envergure ne pouvait qu'avoir bénéficié de l'aide des services russes. Quoiqu'il en soit, si cette attaque a cristallisé le sentiment national estonien et renforcé la société civile dans sa volonté de construire l'État numérique, elle laisse encore aujourd'hui des traces de guerre froide assez vives et il n'est qu'à lire le rapport annuel des services secrets estoniens ou les déclarations des autorités à l'occasion de la présidence estonienne de l'Union européenne pour se convaincre que l'hostilité est frontale. Cette attitude politique est probablement excessive et l'OCDE, dans son rapport sur l'éducation en Estonie, souligne l'importance qu'il y a à donner

aux élèves issus de la minorité russophone les moyens d'accéder aux ressources éducatives. Dans tous les cas, s'inscrire dans une confrontation globale est certes compréhensible, mais elle devra en même temps évoluer, tant l'Europe a besoin d'interfaces lucides, modernes et constructifs avec la Russie. Le fait que des Russes soient aujourd'hui les plus nombreux à demander une e-citoyenneté et que des coopérations s'ouvrent entre l'Estonie et d'autres pays de l'ex-URSS sont probablement des signes d'espoir.

Dans le même temps, le modèle estonien se projette dans un avenir européen, comme en témoignent les collaborations très tôt mises en place avec les pays scandinaves, mais aussi avec le Royaume-Uni ou l'Allemagne. La présidence de l'Union européenne est visiblement un événement majeur pour le pays et toutes les administrations estoniennes ont publié en ligne ce que seront leurs apports à cette occasion. L'Estonie digitale se pense comme une entité européenne pleine et entière et a la fierté de vouloir démontrer au reste de l'Europe qu'elle est un exemple réussi de digitalisation. L'ouverture à la Finlande est logique, celle vers le Luxembourg est plus étonnante et symbolique, le cœur de l'Europe représente une sécurité et un marché pour les citoyens estoniens et un gage de rayonnement mondial à ce qu'ils ont élaboré.

Par ailleurs, l'Estonie digitale est un pays en pleine transition démographique ; le ratio de dépendance est de 28 % aujourd'hui et devrait atteindre 50 % en 2020. Contrairement à l'idée commune d'une résistance à la digitalisation chez les seniors, l'Estonie est un exemple de participation des seniors au marché du travail : le taux d'emploi pour le groupe d'âge des 50-74 ans est de 52 %, contre 42 % dans l'Union européenne des vingt-sept (UE). Si les conditions de santé des personnes âgées sont mauvaises comparées à l'Europe de l'Ouest (25 % des Estoniens entre 50 et 74 ans sont retirés du marché du travail pour des raisons de santé et de dépendance, contre 10 % dans l'UE), dans le même temps, le niveau d'éducation des seniors est très élevé comparé à l'UE et l'accès des seniors à des programmes de formation a été multiplié par six depuis 2005 et est très supérieur à la moyenne de l'UE. L'accès à la formation à tous les âges de la vie est une priorité du gouvernement, sans cesse réitérée depuis 1999.

Enfin, la volonté de coopérer et d'exporter son architecture vers des pays émergents est aussi digne d'intérêt. C'est la démonstration que l'on peut construire un état de droit digital sur une page blanche et qu'il est plus facile de le faire que d'essayer de faire évoluer des structures vieillies et corporatistes. De nombreux pays d'Afrique et d'Asie devraient très certainement pouvoir bénéficier de cette coopération bilatérale – ou sur une base régionale –, dont les apports seront d'autant plus efficaces qu'ils ne seront pas le fruit d'un impérialisme politique ou économique.

Bibliographie

AUERS D., *Comparative Politics and Government of the Baltic States. Estonia, Latvia and Lithuania in the 21st Century*, Department of Political Science, University of Latvia, Palgrave McMillan, 2015.

ERIXON F., "Estonia has Lessons for India's Digital Economy", *livemint.com*, 5 décembre 2017. *http://www.livemint.com/Opinion/x14WEx48oMxeDMkUaVxo2M/Estonia-has-lessons-for-Indias-digital-economy.html*

International Security and Estonia, *valisluureamet.ee*, Estonian Foreign Intelligence Service, 2018.

REYNOLDS M., "'Land is So Yesterday': e-Residents and 'Digital Embassies'", *wired.com*, 17 octobre 2016. *http://www.wired.co.uk/article/taavi-kotka-estonian-government*

NURMELA K. ; OSILA L. ; LEETMAA R., "A Comparative Analysis of the Active Ageing Policies in the Baltic Countries », Praxis, Center for Policy Studies, 2014.

OECD, "Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders", *OECD Public Governance Reviews*, OECD Publishing, Paris, 2015.

OECD, "OECD Economic Surveys: Estonia", OECD Publishing, 2015.

SANTIAGO P. ; LEVITAS A. ; RADO P. ; SHEWBRIDGE C., OECD Reviews of School Resources: Estonia 2016, *OECD Reviews of School Resources*, OECD Publishing, 2016.

ZUBASCU F., "'Digital Revolution' will Underpin Next EU Research Programme says Commissioner", *sciencebusiness.net*, 11 décembre 2017.

La réalité du contexte « cyber »

Eric Filiol

Directeur de recherche

Laboratoire de cryptologie et de virologie opérationnelles, ESIEA

La transformation digitale de nos sociétés est souvent perçue avec crainte, comme un nouveau risque en soi et non simplement comme porteuse de risques – à terme – maîtrisables. Le but de cet article, en adoptant le point de vue de ceux qui doivent non seulement gérer mais également assurer ces risques, est d'expliquer pourquoi, contrairement aux autres révolutions qui se sont produites au cours de l'histoire, un certain nombre d'aspects légitiment ces craintes.

La transformation numérique de la société constitue une nouvelle dimension apparue dans les années 1990. Elle a fait émerger un ensemble de risques et de menaces qui lui sont spécifiques. Cette dimension, improprement (1) nommée « cyber », a pris une place prépondérante dans les sociétés modernes au point que nombreuses sont les interrogations et les inquiétudes à propos de ce qui constitue la dernière révolution en date dans l'histoire de l'humanité [Dugain et Labbé, 2016 ; Mao et Saintourens, 2016]. Toutes les révolutions précédentes – celles de l'imprimerie, de l'industrie, de la médecine, des transports, etc. – ont apporté, même s'il y a eu des périodes d'adaptation, un progrès humain et social ; celle du numérique pourrait bien être celle qui, au contraire, causera sa perte. Un grand nombre d'inquiétudes concerne les impacts sociétaux radicaux tant est fort le sentiment que cette révolution peut potentiellement remettre en question ce que nous sommes fondamentalement. La principale différence de cette révolution tient au fait que le monde numérique est débarrassé de toute limite (temps, espace, potentialités) contrairement au monde physique, cadre unique de toutes les révolutions antérieures.

D'autres inquiétudes concernent une situation de dépendance grandissante à l'égard d'une technologie qui envahit les moindres aspects de notre vie. Notre sécurité, celle de nos biens sont-elles vraiment assurées ? Ces technologies sont-elles fiables ? les maîtrisons-nous véritablement ? Que se passera-t-il quand (et non plus si) des acteurs malveillants en prendront le contrôle ? Autrement dit, quels risques ces technologies du numérique, par leur nature même et par leur omniprésence, font-elles peser sur les sociétés et les individus ?

Au-delà des aspects philosophiques, cet article propose d'analyser et d'évaluer la notion de risque d'une manière certes plus prosaïque mais néanmoins plus concrète et plus pragmatique : celle de l'assureur.

Ce dernier doit assurer ce risque (et éventuellement dédommager la victime). L'activité de tout assureur passe par une analyse préalable du risque (avec in fine une vision actuarielle) ; le but étant de déterminer si le risque est assurable.

Principes généraux

Dans le domaine de la cybersécurité, contrairement aux autres domaines liés par le monde physique, deux grandes classes de risques peuvent être identifiées. La première, relativement bien connue, concerne les risques liés aux technologies elles-mêmes : problèmes de conception, d'implémentation, d'utilisation et de gestion, limites « naturelles » de la technologie, effet des lois naturelles sur les systèmes... L'autre concerne l'environnement lui-même : les attaquants (qui n'existent que dans le domaine de la sécurité) et tous ceux qui définissent, organisent et contrôlent la technologie dans le domaine du numérique, essentiellement les États et les industriels. Cette dernière sous-classe est spécifique au monde de la cybersécurité. Le point fondamental du domaine de la sécurité – cyber ou non – qu'il convient de rappeler est le suivant : la dimension critique est principalement le facteur humain et, par voie de conséquence, celle du droit, dont le but est de gérer l'être humain dans ses interactions avec la société. L'erreur la plus manifeste de la cybersécurité a été de réduire la problématique générale à la seule dimension technique. Cette dernière ne doit pas être l'arbre qui cache la forêt. Un système (électronique, informatique) ne fait pas naturellement d'erreur ou ne constitue pas un risque en soi. C'est son utilisation, sa conception ou sa mise en œuvre qui peut l'être. Elle est donc le fait exclusif de l'être humain.

Par essence, le monde de la sécurité traite de toutes les menaces non prédictibles car adaptatives et ciblées (le fameux duel « épée contre bouclier »). En revanche, le monde de la sûreté concerne les menaces non malveillantes. Ces dernières sont soit le fait des lois de la nature contre le support matériel traitant de l'information (2), soit la résultante d'actions humaines non malveillantes (erreurs). Elles sont par nature prédictibles (modélisées par une ou plusieurs lois de probabilité) et non adaptatives (la menace ne s'adapte pas à la protection).

La non-prédictibilité de la menace dans le domaine de la sécurité impose d'avoir une vision plus large que celle, simplement technique, du scientifique, de l'ingénieur ou du hacker. La dimension véritable est, et doit être, celle du renseignement. Seule la connaissance précise de la victime, de son environnement, de sa façon d'agir et de penser, de travailler, permet à l'attaquant de monter une attaque puissante. Le meilleur exemple d'attaque reposant essentiellement sur une phase de renseignement élaborée est l'usurpation d'identité du dirigeant ou d'un fournisseur. Elle consiste à faire réaliser par l'entreprise un virement bancaire illégitime mais perçu par cette dernière comme légitime [AICPA, 2016].

Cette vision prioritaire – celle du renseignement – est très largement absente de la réflexion du monde de la sécurité. Ce dernier pense encore uniquement en termes de produits et de processus liés à ces produits. Il est fondamental d'adopter la vision russe, qui considère d'abord une cible, puis un ou plusieurs effets à obtenir et, enfin, un champ informationnel large. Dans une moindre mesure, les États-Unis et l'Otan ont, avec le domaine des *information operations* (3) (Info Ops) [JCS, 2014], une vision similaire. Si la réflexion de l'attaquant est nécessairement orientée renseignement, il est important que celle de toute cible ou victime potentielle en soit de même. La vision de l'attaquant est fondamentale, et l'adopter comme principe préalable de défense l'est tout autant.

Les actions purement techniques ou informatiques ne sont qu'une part, non systématiquement nécessaire, du champ des possibles. Seul compte le résultat pour l'attaquant. Et la cible principale reste l'être humain [Filiol et Raynal, 2009 ; Filiol, 2011 ; 2015]. La production effrénée d'informations [Gunelius, 2014] rend cette phase de renseignement

particulièrement simple pour peu que l'on utilise les bonnes méthodes, les bons outils et surtout la bonne vision. À titre d'exemple, la simple analyse de l'empreinte informationnelle des différents membres du comité exécutif d'une entreprise sur les réseaux sociaux suffit pour élaborer une attaque relativement sophistiquée.

L'autre point fondamental dans le domaine de la sécurité est de comprendre que le risque est inévitable. L'attaquant n'est pas modélisable par nature. Il faut se renseigner en permanence sur lui. Il est absurde de penser éviter ou interdire le risque. Les professionnels du marché de la sécurité commettent cette erreur fondamentale. Ce n'est pas l'accumulation de produits plus ou moins compatibles qui permet de gérer systématiquement un attaquant motivé. Il faut considérer que ce risque est inévitable et il convient donc de développer une capacité de résilience. La priorité d'une entreprise n'est pas tant de faire de la sécurité un but en soi mais de créer toutes les conditions pour maintenir son activité, même en conditions dégradées. Autrement dit, il ne faut pas confondre buts et moyens.

Les risques

Les risques technologiques

Ils sont liés aux technologies elles-mêmes, à leur conception, à leur mise en œuvre, à leur gestion et à leur utilisation. Contrairement à l'idée généralement répandue, mais fausse – celle qui voudrait que l'attaquant soit tout-puissant et capable de percer toute défense –, ce n'est pas la force de l'attaquant qui est « dimensionnante » mais la faiblesse, voire l'extrême faiblesse des victimes. L'analyse de très nombreuses attaques contre des entreprises de toutes tailles l'a clairement démontré. L'attaquant – lors de sa phase de renseignement – a recherché et exploité l'existence de faiblesses et de vulnérabilités non prises en compte par la cible (4) [Lecoeuvre, 2015 ; Lagagne, 2011]. Ces « portes » laissées ouvertes sont autant de failles – dans l'organisation, dans les procédures, les contrôles, l'environnement informatique, etc. – que l'attaquant va rechercher et exploiter.

Pour utiliser un parallèle bien connu des assureurs, toute porte laissée ouverte sera inévitablement repérée par un cambrioleur. Et ce n'est pas tant la solidité de la porte blindée qui l'arrêtera (toutes les portes blindées doivent pouvoir être ouvertes par la police – voir section suivante) mais le fait qu'il y en ait une. Il est donc essentiel que toute cible potentielle (entreprise, organisme, personne) établisse la cartographie des vulnérabilités de l'attaquant (vision, phase de renseignement, etc.). Et cela doit être fait non pas comme un absolu en soi mais par rapport à une criticité évaluée et en relation avec l'activité de la cible. Or, cette cartographie n'est pratiquement jamais faite. Dans l'entreprise (5), deux documents essentiels, pourtant encore souvent absents, doivent être systématiquement établis et tenus à jour, et ce avec une vision très large :

- le plan de continuité d'activité (PCA), qui identifie les ressources critiques (hommes, machines, systèmes, procédures, ressources externes (6), etc.) essentielles à l'activité de l'entreprise et répertorie les mesures de tout type à prendre pour maintenir coûte que coûte cette activité ;

- le plan de reprise d'activité (PRA), qui définit les procédures et les mesures à prendre pour revenir à des conditions nominales d'activité après une attaque.

Trop rares sont encore les entreprises ou organismes disposant de PCA/PRA. Parmi de très nombreux exemples, citons le cas des *ransomwares*, ou rançongiciels (virus prenant « en otage » les données de l'entreprise). Depuis quelques années, beaucoup d'entreprises ont subi des dégâts majeurs, voire ont disparu simplement parce que leur politique de sauvegarde des données était déficiente. Ce type d'attaque est devenu une réalité de tous les jours et n'épargne personne. Il est donc essentiel de créer les conditions de survie à une telle attaque. Là encore, l'approche renseignement est fondamentale. La rédaction du PCA doit se faire sous cet angle. Si la loi

de programmation militaire (LPM) 2014-2019 (7), en particulier avec le dispositif SAIV/OIV (8), représente une avancée significative, elle n'est pas suffisante. En effet, elle envisage la menace sous un angle encore trop essentiellement informatique. La résurgence de certains types de terrorisme, très actifs des années 1960 aux années 1990 en Europe (années dites « de plomb »), rend la seule vision informatique illusoire [Filiol et Gallais, 2017]. La question qu'il faut se poser est : l'État dispose-t-il vraiment d'un PCA global et adapté à toutes les formes de menaces ?

Pour illustrer cette réflexion, il est intéressant de considérer l'incident survenu chez OVH, un des opérateurs majeurs dans le monde (hébergement de serveurs, téléphonie, etc.) (9). En novembre 2017, cette entreprise subit une panne électrique majeure (l'entreprise a été victime d'une rupture de service de quelques heures). Un grand nombre d'entreprises, non clientes d'OVH, se sont trouvées impactées, de manière conséquente pour certaines. En effet, elles dépendaient de services (par exemple des systèmes connectés d'ouverture d'accès) dont les prestataires, eux, avaient installé leurs serveurs chez OVH (10). La faute n'est pas imputable à OVH, qui ne pourra jamais empêcher les attaques mais seulement en minimiser les effets. La faute est imputable aux entreprises qui n'ont pas établi la cartographie de leurs dépendances fonctionnelles externes (11). Le cas des attaques de l'été 2017 par des virus destructeurs (*wipers*), WannaCry et NotPetya, est aussi un exemple frappant. Ces attaques ont fait des dégâts considérables dans des entreprises au niveau mondial (Saint-Gobain, Maersk, FedEx, Renault...). Ces sociétés n'avaient pris en compte que la sauvegarde des données (données traitées) et non celle des systèmes et des fonctionnalités (données et systèmes traitants), pourtant critiques pour elles autant que les données. Là encore, la réflexion PCA était incomplète et insuffisante.

Les risques liés à l'environnement

La transformation digitale de la société s'est faite extrêmement rapidement et d'une manière incontrôlée. En dix ans, un nombre croissant de technologies ont pris place dans notre environnement, de sorte que nous avons développé une situation de totale dépendance sans nous assurer que cette dépendance pourrait être fatale. Cette transformation subite et non maîtrisée a créé un contexte défavorable, porteur de risques très élevés et très difficiles à gérer. Ces risques sont principalement au nombre de trois (12).

Le premier concerne une carence grandissante de spécialistes dans le domaine, tant juniors (capables techniquement de faire le travail) que seniors (capables de gérer une équipe tout en étant légitimes, auprès de leurs subordonnés, sur le plan technique). On estime généralement qu'il faudra vingt ans pour former ces spécialistes en quantité suffisante (13). Cette situation est due au fait que les préoccupations de sécurité sont récentes. Le label SecNumedu de l'Agence nationale de la sécurité des systèmes d'information (Anssi), avancée très significative, n'a vu le jour qu'en 2017 (14). Jusqu'à récemment, voire encore actuellement, la cybersécurité était absente des programmes d'enseignement supérieur en informatique et dans la plupart des cahiers des charges de projets. Cette hypertension dans le recrutement des profils dans ce domaine s'accompagne malheureusement des conséquences habituelles dans pareilles situations : baisse de la qualité des personnels, comportements peu vertueux (salariés prêts à se vendre au plus offrant), etc. Enfin, la criticité de certains postes (administrateur réseaux, responsable de la sécurité des systèmes d'information – RSSI, *data protection officer* – DPO, auditeur de sécurité, etc.) devrait rendre obligatoire une habilitation spécifique pour ces personnels au pouvoir étendu, voire total, sur le système d'information. Cette réflexion n'a toujours pas abouti auprès des pouvoirs publics.

Le second risque concerne la souveraineté dans le domaine des technologies. L'hégémonie technologique, commerciale et stratégique de deux blocs (les USA pour les logiciels et les services, la Chine pour le matériel) ne permet pas au reste du monde de maîtriser sa propre sécurité. Les révélations, fréquentes depuis 2013 (Snowden, fuites de la NSA, de la CIA et de Microsoft), montrent clairement que cette

hégémonie est utilisée par ces blocs pour espionner et maintenir un état d'insécurité globale à leur avantage. Toute cybersécurité est illusoire dès lors qu'elle utilise les outils fournis par l'adversaire [Filiol, *in* Le Dain et Sido, 2015 ; Filiol, 2013].

Le troisième et dernier risque, et non des moindres, est lié à la position équivoque des États. Ces derniers voient dans cette transformation digitale une opportunité pour exercer plus facilement, à moindre coût et avec beaucoup moins de contrôles par les autorités judiciaires et les autorités administratives indépendantes (AAI) comme la Cnil, des activités de police et de renseignement. Cette situation est de nature à remettre en cause les libertés et les valeurs fondamentales d'une démocratie (15). Les États organisent, dans une certaine mesure, un contexte d'insécurité numérique permanente. Ils sont donc pris dans une schizophrénie sidérante : ils doivent respect et protection aux citoyens tout en conservant la capacité de contrôler les acteurs les plus malfaisants. Les récentes propositions par le ministre de l'Intérieur français en 2017 illustrent parfaitement cette tendance dangereuse. Il souhaitait, d'un commun accord avec son homologue allemand, que soient systématiquement installées des portes dérobées dans les moyens de chiffrement. Or, ces derniers sont au cœur de toute sécurité.

Que conclure de tout cela ? La notion d'assurance des risques dans le domaine de la cybersécurité est-elle viable et a-t-elle même un sens ? Le doute est permis, car certains risques liés au contexte ne sont pas forcément maîtrisables. Mais il convient surtout de garder à l'esprit ce qui fait l'essence même du domaine informatique. Contrairement au domaine physique (un accident de voiture ou un sinistre incendie), trois facteurs importants lors d'une analyse de sinistre peuvent disparaître dans le cas d'une attaque informatique : le temps, l'espace et, surtout (quand l'attaquant est compétent), la capacité de preuve. L'imputabilité même d'une attaque est quelquefois impossible. Il est donc essentiel que la vision de l'assureur, encore trop absente, soit systématiquement privilégiée car c'est elle qui peut permettre, tant sur le plan technique qu'au niveau politique, d'apporter la maturité suffisante à un domaine encore trop jeune et trop mal maîtrisé.

Notes

1. La cybernétique, née des travaux de Norbert Wiener, décrit la vision unifiée des domaines naissants de l'automatique, de l'électronique, de la théorie mathématique de l'information et, de fait, concerne plus la robotique voire l'intelligence artificielle [Wiener, 1948].

2. Il est important de noter que l'existence d'un support matériel caractérise le risque et la nature de la menace. Une information n'existe que dans la mesure où elle est représentée par un support (papier, flux d'électrons ou de photons, atmosphère, support magnétique...). Sans support, on ne parle pas d'information mais d'idée. Le simple fait d'énoncer une idée (par la voix) en est l'expression la plus simple (vibrations mécaniques de l'air, lesquelles peuvent être écoutées).

3. Les « opérations d'information » (Info Ops) constituent un ensemble de techniques de guerre électronique mises en œuvre par l'armée dans le but d'affecter les systèmes d'information adverses tout en défendant ses propres systèmes d'information. Elles incluent des actions sur les réseaux informatiques (CNO) ainsi que des opérations de manipulation psychologique (Psy Ops), de désinformation militaire (MIL-DEC) et de sécurisation intérieure (Opsec).

4. Voir aussi l'article du blog L'Observeur : http://www.synthese-informatique.com/le-blog/derniers-articles-publies/entry/info-dsi/selon-9-rssi-sur-10-les-failles-de-donnees-dont-ils-ont-connaissance-ne-sont-pas-traitees

5. Il est intéressant de noter que cette réflexion est tout aussi importante dans le domaine familial et privé. Combien de familles sont particulièrement vulnérables à une panne générale d'électricité ou d'eau, à une rupture conséquente et

prolongée d'approvisionnement dans les magasins, etc., en particulier dans les grandes villes. Jamais la résilience des populations urbaines n'a été aussi faible qu'aujourd'hui. Peu de gens sont conscients de l'extrême fragilité de nos sociétés dites modernes, plus que jamais dans notre histoire. Toute famille devrait avoir son propre PCA.

6. Filiol et Raynal [2009].

7. https://www.ssi.gouv.fr/administration/protection-des-oiv/protection-des-oiv-en-france/

8. SAIV/OIV : sécurité des activités d'importance vitale/ opérateurs d'importance vitale.

9. http://www.zdnet.fr/actualites/panne-ovh-incident-clos-et-premieres-explications-techniques-39859778.htm

10. http://www.linternaute.com/actualite/societe/1417756-ovh-les-sites-de-bfm-nexity-01net-en-panne-comme-des-centaines-d-autres/

11. Voir par exemple Filiol et Raynal [2009].

12. Un quatrième risque que nous ne développerons pas ici, faute de place, concerne la fracture numérique qui s'installe dans nos propres pays dits modernes. Cette fracture a des conséquences dramatiques auprès des populations fragiles (personnes âgées, déclassés sociaux, etc.), qui sont de fait exclues peu à peu et mises en danger.

13. Cette estimation considère que les technologies vont continuer à apparaître et à évoluer au même rythme, avec le taux d'attrition ou d'obsolescence des personnels actuel, et que le temps de formation n'est pas immédiat. Il faut cinq ans a minima pour former un ingénieur junior.

14. https://www.ssi.gouv.fr/entreprise/formations/secnumedu/

15. http://www.slate.fr/story/114869/sicard-justice-etat-urgence-decheance

Bibliographie

AICPA, *FVS Eye on Fraud*, n° 1, été 2016. Disponible en PDF : *https://www.aicpa.org/InterestAreas/ForensicAndValuation/Resources/FraudPreventionDetectionResponse/DownloadableDocuments/fvs-eye-on-fraud-newsletter-summer-2016.pdf*

Dugain M. ; Labbé C., *L'homme nu. La dictature invisible du numérique*, Robert Laffont – Plon, 2016.

Filiol E., « Comment vraiment paralyser un pays à l'aide du cyber », *Les Cahiers de la Revue Défense Nationale*, « Penser autrement », 10 juin 2015, pp. 103-110.

Filiol E., texte d'audition devant la commission parlementaire, *in* Le Dain A.-Y. ; Sido B., « Sécurité numérique et risques : enjeux et chances pour les entreprises », rapport n° 2541 (Assemblée nationale)/n° 271 (Sénat) de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), tome II, 2 février 2015, pp. 181-188.

Filiol E., "The Control of technology by Nation States: Past, Present and Future – The Case of Cryptology and Information Security", *Journal of Information Warfare*, vol. 12, n° 3, octobre 2013, pp. 1-10.

Filiol E., « Renseignement, planification et conduite d'une cyberattaque », *in* Ocqueteau F. (dir.), « Contrôles et surveillance dans le cyberespace », *Problèmes politiques et sociaux*, n° 988, septembre 2011, La Documentation française, p. 69ff.

Filiol E. ; Gallais C., "Combinatorial Optimization of Operational (Cyber) Attacks against Large-scale Critical Infrastructure. The Vertex Cover Approach", *International Journal in Cyber Warfare and Terrorism*, vol. 7, n° 3, juin-juillet 2017, pp. 29-43.

Filiol E. ; Raynal F., « Cyberguerre : de l'attaque du bunker à l'attaque dans la profondeur », *Revue Défense Nationale*, n° 717, mars 2009, pp. 74-86.

Gunelius S., "The Data Explosion in 2014 Minute by Minute", *aci.info*, 12 juillet 2014. Lien : *http://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/*

Joint Chiefs of Staff (JCS), "Information Operations", Joint Publication 3-13, 2014. Disponible en PDF : *https://fas.org/irp/doddir/dod/jp3_13.pdf*

Lagagne C., « L'attaque de Bercy : "Un mal pour un bien" selon Check Point », *silicon.fr*, 7 mars 2011. Lien : *https://www.silicon.fr/lattaque-de-bercy-%c2%ab-un-mal-pour-un-bien-%c2%bb-selon-check-point-46939.html?inf_by=5a6dab2c671db8290d8b4fe3*

LECOEUVRE S., « Les mots de passe de TV5 Monde dévoilés sur France 2 », *tvmag.lefigaro.fr*, 10 avril 2015. Lien : *http://tvmag.lefigaro.fr/le-scan-tele/insolite/2015/04/10/28009-20150410ARTFIG00214-les-mots-de-passe-de-tv5-monde-devoiles-sur-france-2.php*

MAO B. ; SAINTOURENS T., *Cyber fragiles. Enquête sur les dangers de nos vies connectées*, Tallandier, 2016.

WIENER N., *Cybernetics: Or Control and Communication in the Animal and the Machine*, John Wiley & Sons, 1948.

Les données un patrimoine à protéger

Laure Zicry

Head of Cyber, Western Europe, Gras Savoye Willis Towers Watson

Comme jadis on protégeait ses biens contre les cambriolages ou les simples effractions, depuis quelques années, c'est contre les cyberattaques que l'on doit se prémunir. Et quelle est la première motivation des pirates informatiques ? Les données ! En sus du patrimoine mobilier et immobilier qui constitue l'actif de l'entreprise, il y a désormais un nouveau patrimoine à protéger, le patrimoine informationnel, et celui-ci se développe à grande vitesse avec la digitalisation. Les données sont devenues un enjeu majeur pour l'entreprise et elles attirent la convoitise.

Le *risk manager* doit non seulement protéger son entreprise contre le vol de données, lesquelles constituent par essence un bien intangible mais dont la valeur est bien plus importante que le contenant dans lequel elles sont stockées, mais aussi se doter de mesures de protection des systèmes d'information et de détection des intrusions qui lui permettront d'être informé des tentatives d'intrusion ainsi que des intrusions ayant permis le vol de données.

La difficulté majeure réside dans le fait que bon nombre d'entreprises ne découvrent qu'après des mois que des tiers ont eu accès à un système de traitement automatisé des données (Stad) et que les données, même si elles ont été dérobées, n'ont pas pour autant disparu des systèmes d'information. Le pirate informatique les aura tout simplement copiées ou aura agi de manière que les traces de son intrusion dans les systèmes d'information soient masquées.

La tâche est donc particulièrement ardue mais à la fois intéressante à traiter. On est loin ici des risques traditionnels d'incendie et d'explosion ou de ceux liés au transport de marchandises, pour lesquels l'aléa, lorsqu'il survient, est visible, concret, avec des conséquences directes quasi immédiates. Le défi du *risk manager* est double : il doit protéger son entreprise contre les cyberattaques, et ce afin de protéger les données. En effet, lorsqu'une entreprise se fait attaquer, elle est victime de l'attaque, mais elle n'en reste pas moins responsable vis-à-vis des tiers.

Quelles sont les données à protéger et pourquoi ?

Pour mettre en œuvre les mesures de protection les plus adéquates, il faut identifier les différents types de données et appréhender leur valeur. Chaque donnée a une valeur pour l'entreprise qui la détient, mais il faut aussi avoir conscience que celle-ci a une tout autre valeur pour celui qui la vole. Ainsi, trois grandes catégories de données doivent être protégées : les données à caractère personnel, les données confidentielles et les données métiers ou de gestion.

Données à caractère personnel

Les premières auxquelles tout le monde pense immédiatement sont les données à caractère personnel. Leur protection doit être assurée depuis le 6 janvier 1978, date de la promulgation de la loi Informatique et libertés et date de création de la Commission nationale de l'informatique et des libertés (Cnil), qui en est la garante.

La Cnil dispose de pouvoirs de contrôle, d'enquête et de sanction. Ce dernier a d'ailleurs été modifié en octobre 2016 par la loi pour une République numérique, avec un plafond maximal des sanctions (qui peuvent être prononcées en cas de manquement – à la loi – et d'avantages tirés de ce manquement) porté à trois millions d'euros.

Dès octobre 2011, la loi Informatique et libertés a été renforcée du fait de la transposition du « paquet télécoms ». En effet, depuis cette date, les fournisseurs d'accès à Internet et les fournisseurs de services de téléphonie fixe et/ou mobile se sont vus contraints de notifier à la Cnil mais aussi aux personnes concernées toutes les violations de données à caractère personnel sous peine de sanction.

L'article 34 bis de la loi Informatique et libertés définit la « violation de données à caractère personnel » comme toute violation de la sécurité entraînant, accidentellement ou de manière illicite, la destruction, la perte, l'altération, la divulgation, ainsi que l'accès non autorisé à celles-ci, des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communication électroniques.

Le 27 avril 2016, le règlement général sur la protection des données (RGPD) était promulgué. Son entrée en vigueur est attendue pour le 25 mai 2018. Celui-ci ne fera pas l'objet d'une transposition dans les droits nationaux puisqu'il s'agit d'un règlement européen et non d'une directive. Toutefois, certaines dispositions de la loi Informatique et libertés existantes devront être modifiées et c'est la raison pour laquelle un projet de loi a été déposé.

À l'instar du « paquet télécoms », le RGPD prévoit que les entreprises publiques comme privées devront informer l'autorité nationale en charge de la protection des données (en France, la Cnil) à la suite d'une violation de données à caractère personnel. Cette notification devra être réalisée dans des délais très courts (dans les 72 heures suivant la connaissance de la violation de la confidentialité).

Le contenu de la notification est également encadré par le RGPD. Les sanctions en cas de manquement à cette obligation de notification sont très lourdes et peuvent atteindre 4 % du chiffre d'affaires du groupe, avec un minimum de 20 millions d'euros.

Données confidentielles

Les données confidentielles doivent elles aussi faire l'objet d'une protection particulière, du fait même de leur caractère confidentiel. Soit cette confidentialité est prévue contractuellement (marché, contrat ou engagement contenant une clause de confidentialité), soit celle-ci découle de la loi (secret professionnel notamment), soit c'est l'entreprise elle-même qui choisit de classifier certaines données qui ne relèvent ni de la première catégorie ni de la seconde.

Dans ce dernier cas, les données étant considérées comme particulièrement sensibles, un nombre restreint d'employés doit pouvoir y accéder.

Données métiers ou de gestion

Enfin, les données métiers ou de gestion ne sont ni des données à caractère personnel ni des données confidentielles, mais elles représentent des informations très importantes pour l'entreprise, qui, en leur absence, ne peut pas fonctionner. Ici on peut citer les données métiers qui permettent de configurer des machines, des outils de production ou même des systèmes d'information (tel le *Supervisory Control and Data Acquisition*, plus connu sous le nom de Scada). Quant aux données de gestion, elles doivent également être protégées, car, sans celles-ci, l'entreprise ne pourrait pas régler les factures ni payer ses salariés.

Une fois les données de l'entreprise identifiées (voire classifiées), il faut en connaître la valeur. Et, sur ce point, nous sommes face à une contradiction. Les entreprises ne savent généralement pas chiffrer la valeur des données qu'elles détiennent et n'ont bien souvent aucune idée du prix qui s'y attache ou, sinon, le sous-estiment. Combien d'entreprises pensent qu'elles ne peuvent pas être attaquées, car les données détenues dans leurs systèmes d'information n'ont selon elles aucune valeur ! Combien se disent qu'elles ne peuvent pas être attaquées car, ne faisant pas partie des grands groupes mondialement connus, elles ne sont pas visibles ? Que d'erreurs commises, que de méconnaissance... Cependant, pour les pirates informatiques, rien n'est plus clair ! Les données sont en général revendues sur l'Internet clandestin (Dark Web), où les prix sont fixés. Il y a même, comme dans la vie réelle, des périodes de soldes !

Il n'y a pas de secteurs ou d'industries types qui sont plus visés que les autres, il y a toutes les entreprises qui sont mal protégées et qui possèdent toutes des données. Voler ces dernières, les rendre indisponibles ou leur faire perdre leur intégrité portera un coup dur, voire fatal, à l'entreprise (et, sur ce point, les grands groupes s'en relèveront bien mieux que les PME).

Toutefois, en fonction du type des données, ce ne sont pas les mêmes risques qui seront identifiés.

À quoi s'attendre ?

Appréhender les risques qui pèsent sur l'entreprise, c'est l'autre étape à mener et qui peut être concomitante de celle de l'identification des données à protéger. Le *risk manager* doit réaliser une cartographie des risques et ainsi comprendre comment il doit se protéger contre toute problématique de disponibilité, d'intégrité, de confidentialité ou de traçabilité de la donnée.

Le risque cyber n'a pas de frontière, il ne peut pas être circonscrit à un pays ou à un système d'information. En effet, l'interconnectivité des réseaux démultiplie les risques d'atteinte aux systèmes d'information et donc d'atteinte aux données. Les cyberattaques peuvent venir de n'importe où, et il existe différentes méthodes d'attaque (*phishing*, virus, attaque DoS/DDoS (1), etc.). L'année 2017 a été marquée par deux grandes attaques mondiales avec des impacts significatifs sur le bilan des victimes de WannaCry en mai ou de Not/Petya en juin.

Les campagnes de *ransomwares* sont courantes depuis plusieurs années, et la France a fait partie des pays les plus touchés avec les *cryptolockers* Locky ou Dridex. Toutefois, WannaCry n'est pas un *ransomware* comme les autres. La particularité de WannaCry réside dans sa vitesse de propagation (2) dans les systèmes à travers le monde. Des milliers de serveurs à travers la planète ont été infectés, et, en l'espace de deux jours, des entreprises du monde entier ont déclaré avoir été touchées. L'interconnexion des réseaux informatiques a aussi été un facteur de succès de l'épidémie.

Quant à Not/Petya, il a infesté des milliers d'entreprises de toute taille dans la nuit du 27 juin 2017. Il ne s'agissait pas d'un *ransomworm* comme l'était WannaCry mais d'un virus destructeur qui a obligé bon nombre d'entreprises à repenser totalement leur système d'information. Le CEO de Maersk, l'une des plus grandes entreprises de transport au monde, a déclaré que le groupe avait dû réinstaller 45 000 PC et 4 000 serveurs.

Les dégâts occasionnés sont gigantesques, et les impacts sur le bilan des entreprises non négligeables. Maersk a estimé les dégâts causés par Not/Petya entre 250 millions et 300 millions d'euros. Le géant pharmaceutique Merck ainsi que FedEx ont eux aussi déclaré des pertes qui se chiffrent en millions d'euros.

La France n'a pas été épargnée par ces deux vagues d'attaques, et de grands groupes se sont ainsi vus paralysés pendant plusieurs jours voire plusieurs semaines, le temps de décontaminer les serveurs ainsi que les postes de travail.

Il existe un autre risque important qui ne doit pas être négligé : le risque humain. À l'instar d'autres risques, le facteur humain est souvent la cause du dommage ou à tout le moins y contribue. On croit souvent qu'il suffit de se prémunir contre les pirates informatiques, mais il ne faut pas oublier le risque que représentent les salariés. La négligence des employés est le facteur de risque le plus important. Les attaques par *phishing* sont très courantes, et c'est bien par la négligence du salarié que le virus va s'introduire dans les systèmes et contaminer l'ensemble des serveurs et postes de travail. On peut aussi citer l'acte malveillant d'un salarié mécontent ou en conflit avec son employeur susceptible de causer des dommages non négligeables à l'entreprise.

Le niveau de maturité en termes de sécurité informatique et de connaissance du risque est un élément fondamental dans la protection des données. Les risques sont bien réels, et le *risk manager* a souvent recours à l'assurance.

S'assurer contre les cyberattaques pour mieux protéger ses données, c'est le pas qu'ont déjà franchi un grand nombre de *risk managers*. Ils ont vu dans le transfert du risque à l'assurance un gain pour l'entreprise et une meilleure protection du bilan. La protection des données étant un sujet majeur, il faut s'attendre à ce que le renforcement législatif et réglementaire décrit plus haut couplé à des attaques de plus en plus courantes ait un impact significatif sur le marché de l'assurance cyber.

Notes

1. DoS/DDoS : Denial of Service/Denial Distributed of Service. *En français : déni de service/déni de service distribué.*

2. D'ailleurs, pour être plus précis, WannaCry n'est pas un ransomware *mais un* ransomworm*, un ver qui a la particularité de se propager très rapidement.*

Placer l'humain au cœur de la cybersécurité

Arnaud Tanguy

Chief Information Security Officer, AXA Investment Managers

Président du groupe de travail Cybersécurité et procédures, AFG (1)

Maîtriser sa cybersécurité est un enjeu majeur dans un monde en profonde transformation numérique, c'est pourquoi les entreprises se dotent de moyens grandissants pour se protéger : ressources dédiées, acquisition d'outils et de logiciels, renforcement de la gouvernance et des contrôles de sécurité. Une des dimensions essentielles d'un dispositif de sécurité efficace réside dans la sensibilisation des collaborateurs et la mobilisation de leur attention. Placer l'humain au cœur du dispositif est capital, notamment parce que les erreurs humaines se trouvent à l'origine de la plupart des cyberattaques récentes. Beaucoup d'entreprises l'ont compris et ont entamé, depuis de nombreuses années, des démarches de sensibilisation de leurs collaborateurs visant à leur faire adopter de bonnes pratiques en matière de sécurité.

Toutefois, les approches classiques d'éducation et de formation atteignent aujourd'hui leurs limites car elles ont tendance à réduire la sécurité de l'information à un sujet technique et contraignant. De ce fait, les utilisateurs ne s'approprient pas complètement les règles, voire les outrepassent volontairement. Il est donc nécessaire de faire évoluer ces approches en développant une culture de la cybersécurité, afin d'obtenir un changement profond et durable du comportement des collaborateurs et de faire de l'humain le meilleur allié de la protection de l'entreprise.

Le facteur humain au cœur des cyberméfaits

La majorité des grands piratages récents (2) ont une cause humaine directe ou indirecte. Choix de mots de passe à faible niveau de sécurité, clic sur une fausse publicité, ouverture d'un e-mail de *phishing* (3) ou envoi d'un e-mail au mauvais destinataire sont autant d'actions qui peuvent avoir des conséquences dramatiques pour une société.

Quelle que soit leur motivation, les attaquants tentent systématiquement d'utiliser les faiblesses humaines pour perpétrer leurs méfaits. Si une attaque vise une organisation, l'ensemble des collaborateurs, consultants, partenaires voire clients deviennent des cibles potentielles pour accéder à des systèmes, voler des informations ou rendre indisponibles des systèmes en échange d'une rançon.

Les techniques de sensibilisation et de responsabilisation des utilisateurs et des employés prouvent toute leur valeur dans deux des grandes causes de

cyberattaque qui impliquent l'humain : l'ingénierie sociale (4) et les négligences des utilisateurs.

La mise en œuvre d'un tel programme peut ainsi contribuer grandement à prévenir ces risques. La plupart des employés ne savent pas comment identifier un individu malveillant ou ignorent les signaux à surveiller. Donner des clés et des techniques pour identifier un faux appel téléphonique, mais surtout rappeler les bonnes pratiques permet d'éviter les négligences des utilisateurs qui peuvent entraîner des cyberattaques d'envergure ou une fuite d'information involontaire.

Il permet également de mobiliser toute l'entreprise, non seulement les équipes chargées de la sécurité de l'information ou de l'informatique mais aussi, et surtout, les dirigeants et l'ensemble des collaborateurs en créant une véritable culture de la cybersécurité.

Former et sensibiliser autrement

La plupart des entreprises mettent déjà en œuvre des actions ou des plans structurés de sensibilisation et de formation des collaborateurs. Cette approche, qui martèle depuis les années 2000 que « la sécurité est l'affaire de tous », à savoir que la sécurité de tous réside dans les mains de chacun, atteint aujourd'hui ses limites.

En effet, cette démarche s'articule principalement autour du rabâchage des règles obligatoires dans les entreprises, généralement compilées sous la forme d'une « politique de sécurité de l'information ». Cette étape est bien entendu incontournable, mais la connaissance de ce corpus documentaire, imposée au salarié, parfois via son contrat de travail ou le règlement intérieur de l'entreprise, n'est pas bien assimilée. Comme pour tout contrat, l'entreprise se doit donc d'en communiquer le contenu. Pour certaines professions réglementées, en particulier dans les secteurs financier ou de la santé, la sensibilisation des collaborateurs est même une obligation réglementaire. Cette approche obligatoire, voire souvent contrainte, conduit au désintérêt et parfois au désengagement des collaborateurs. Les actions de sensibilisation ont tendance à aborder la sécurité sous un angle technique : créer un mot de passe complexe, chiffrer les documents confidentiels, utiliser un logiciel sécurisé pour se connecter au réseau de l'entreprise. Même si cette pratique reste nécessaire, elle n'est pas suffisante : en réduisant la sécurité à sa dimension technique, on exclut les employés technophobes.

Ces règles sont répétées depuis de nombreuses années, et les utilisateurs les connaissent généralement, mais ce n'est pas pour autant que ceux-ci les appliquent. Non accompagnées d'explications sur la nature des risques ou de communications à propos des tentatives de cyberattaque, les règles de sécurité sont souvent perçues comme une contrainte, un frein à la productivité. Et comme ces règles sont décorrélées de la notion de risques, les utilisateurs ne comprennent simplement pas pourquoi ils doivent les appliquer ; ils peuvent même avoir le sentiment d'être surveillés devant l'accumulation de dispositifs de contrôle et de détection d'incidents.

C'est un paradoxe fort : alors que l'on demande aux employés d'être toujours plus agiles et inventifs, ceux-ci ont l'impression que les règles qu'ils doivent appliquer freinent l'innovation et la rapidité d'exécution. Ainsi, les employés et les utilisateurs deviennent des boucs émissaires idéaux : on leur demande d'être la première ligne de défense de la sécurité informatique et dans le même temps de tirer parti de tous les outils numériques à leur disposition afin d'être efficaces et réactifs face au flot continu d'informations qu'ils ont à traiter. Cela aboutit souvent à un clic malheureux ou à une situation de risque pour l'entreprise.

Face à l'évolution numérique de la société, la sécurité doit accompagner les entreprises dans leurs mutations et replacer l'humain au cœur du dispositif. Il faut inscrire cette logique d'éducation nécessaire dans une démarche plus large de changement culturel autour de la sécurité.

Vers un changement culturel autour de la sécurité

Ces dernières années, l'agilité et la transformation des entreprises ont engendré des cycles d'évolution beaucoup plus courts tant du point de vue des métiers ou des usages qu'au niveau des technologies. Tous les jours, de nouveaux outils apparaissent. À titre d'exemple, un utilisateur moyen utilise près de 40 applications par mois sur son smartphone (5).

Il est ainsi illusoire de vouloir fournir des règles de sécurité pour chaque évolution ou nouvelle technologie. Il faut pouvoir transmettre des principes applicables largement et des réflexes de prudence permettant d'adopter un comportement de sécurité dans toutes les situations.

Illustrer concrètement les risques

Même si plus personne ne peut occulter ni éviter les grands titres des journaux faisant état des cyberattaques, les utilisateurs ne sont pas toujours conscients des risques dans le cadre de leur activité. Ils ont le sentiment d'être protégés par les dispositifs techniques et les moyens mis en œuvre par leur entreprise. Ils sont souvent moins vigilants dans leur environnement de travail que dans leur cadre personnel.

Cela constitue réellement un premier axe de travail pour les entreprises : il faut expliquer aux salariés les risques auxquels ils peuvent être exposés et les illustrer concrètement. Par exemple, on peut s'appuyer sur l'actualité en détaillant comment un piratage a causé l'indisponibilité des moyens informatiques, comment un clic sur un e-mail de *phishing* a entraîné la divulgation d'informations sur les clients ou a abouti à une amende de la part d'un régulateur. Il faut ainsi rappeler que, malgré les dispositifs techniques en place, l'attention et la vigilance de tous sont nécessaires et que tout écart peut exposer gravement le salarié, la société et les clients.

Un des enjeux clés ici est de trouver les bons exemples en fonction de l'activité de la personne ; on parle ici de technique de segmentation des cibles.

Adopter des techniques de segmentation marketing

Tout comme dans une approche marketing, il est important de bien cartographier et de segmenter les populations concernées afin d'adapter les messages et les canaux d'information aux enjeux respectifs de celles-ci. On distingue généralement au moins trois catégories d'utilisateurs nécessitant une attention particulière : la direction générale, les opérationnels de l'informatique et du numérique et l'ensemble des collaborateurs. Mais on doit ajouter à celles-ci les populations considérées comme sensibles du fait de leur activité ou de la nature des informations qu'elles manipulent ; il peut s'agir de la direction des ressources humaines, des équipes chargées des fusions-acquisitions, des équipes commerciales.

L'implication de la direction est aujourd'hui un des facteurs clés de l'adoption et de la généralisation d'une culture de la cybersécurité encourageant chacun à adopter des comportements sécuritaires dans son activité quotidienne. Les études (6) démontrent que les entreprises dans lesquelles les cadres supérieurs vivent et incarnent une culture de sécurité ont un niveau d'adoption supérieur.

Transformer l'image de la sécurité

Ne le nions pas, la perception de la sécurité était historiquement négative et abstraite. Dans l'imaginaire collectif, il s'agit d'un sujet sérieux, technique et souvent compréhensible uniquement par des experts au jargon obscur et inintelligible.

Pour retenir l'attention des collaborateurs, il est nécessaire de simplifier les messages et de fédérer les collaborateurs autour de thèmes en relation avec leur activité et celle de l'entreprise. Il faut travailler une accroche et une image, partager une vision commune

qui récapitule les grandes missions et qui sert de fil conducteur à une campagne annuelle. Une bonne culture de la cybersécurité ne s'instille que si elle est alignée avec la culture d'entreprise ; culture de la performance, culture du processus, culture de la créativité, autant de valeurs à creuser pour partager ces sujets.

Jouer la carte de l'interactivité

Le temps des présentations magistrales sans interactivité ou des notes de service transmises par messagerie est révolu. Un des maîtres mots d'une sensibilisation réussie doit être l'interactivité. Cela peut se faire sous la forme d'ateliers ou d'événements d'entreprise thématiques avec des démonstrations de piratage, par exemple. Lorsque les participants découvrent qu'il est facile pour un pirate de prendre le contrôle de la webcam d'un poste de travail de démonstration en y connectant simplement une souris modifiée, vous assurez un « buzz » généralisé dans l'entreprise.

Il faut jouer la carte du collaboratif et de l'innovation. Plutôt que d'avoir un questionnaire papier où chacun évalue ses connaissances en matière de cybersécurité, on peut imaginer un questionnaire interactif via une application sur smartphone qui met en compétition, en temps réel, les participants et qui génère immédiatement attention et intérêt.

Une autre action très interactive, et à l'impact significatif, consiste à simuler des attaques de *phishing*. Via l'envoi d'e-mails, les collaborateurs sont invités à cliquer sur un lien ou à ouvrir une pièce jointe. Cela illustre concrètement les précautions à prendre vis-à-vis du courrier électronique.

Établir un pont entre la sécurité dans l'entreprise et la protection de sa vie privée

Cette sensibilisation à la sécurité est fondamentale à chaque instant de la vie, et pas seulement dans le cadre professionnel. Dans un monde de plus en plus numérique, les individus sont exposés dans leur vie personnelle aux mêmes cybermenaces : hameçonnage, usurpation d'identité, vol ou destruction des données privées, ou encore gestion des mots de passe... En mettant en lumière les risques liés à la cybersécurité sous l'angle de la vie privée et de l'impact émotionnel et humain qu'ils peuvent générer dans le cercle familial, les employés sont plus engagés.

La sensibilisation d'entreprise, en expliquant les règles applicables au sein d'une société doit également répondre aux préoccupations personnelles de l'employé, telles que la façon de mieux protéger ses finances personnelles, son environnement familial et, de manière plus large, son identité, qui est de plus en plus numérique.

Sortir des sentiers battus

Comment parler de sécurité sans en avoir l'air ? Le format des conférences thématiques s'y prête parfaitement. Inviter un conférencier prestigieux à s'exprimer à propos d'un sujet sans rapport apparent avec la sécurité s'avère efficace pour évoquer cette dernière sous un angle différent et original. Voici quelques exemples réels, non exhaustifs, de thèmes de conférence porteurs de ces objectifs de sensibilisation.

Inviter un neuroscientifique pour détailler les ressorts fondamentaux du cerveau ou un « mentaliste » qui, sur scène, utilise les techniques des manipulateurs et des illusionnistes permet au final de décrypter les risques en matière de manipulation et d'ingénierie sociale utilisées par les pirates et de mettre en évidence les bonnes pratiques.

Inviter un philosophe spécialiste des séries de la pop culture permet d'exposer, de démontrer comment la fiction et la culture populaire au travers des séries ou des films s'imprègnent des notions de cybermenaces et de piratage. Une telle démonstration permet de clarifier interactivement avec la salle ce qui relève de la fiction ou de la réalité et la façon de se prémunir.

Pour faire comprendre la réalité de l'intérieur d'une cyberattaque, quoi de plus efficace qu'inviter le dirigeant d'une société ayant subi une perte d'activité temporaire. Un témoignage sincère et vivant, qui détaille les ressorts humains et émotionnels d'un piratage d'envergure, interpelle directement l'auditoire sur le rôle que chacun a à jouer pour se protéger collectivement.

Un excellent ratio coût/efficacité

Un tel programme ne s'improvise pas et doit être planifié et budgété. Un plan de sensibilisation simple basé sur des initiatives peut certes être mis en œuvre à moindre coût par des collaborateurs internes et des partenariats avec vos prestataires de services de sécurité. Les programmes ambitieux nécessitent des enveloppes conséquentes, mais le retour sur investissement est important. Comme le montre l'enquête annuelle sur la sécurité de l'information menée par l'Association française de la gestion financière (AFG), le ratio investissement/efficacité (7) d'une campagne de sensibilisation est l'un des meilleurs comparé à celui de tous les autres dispositifs de sécurité. Si le coût d'un programme de sensibilisation reste important, il est toutefois moins élevé que celui des licences des solutions techniques, et le retour sur investissement est supérieur.

Considérées par le passé comme un sujet d'expert, pour lequel on attendait que les individus se contentent d'apprendre et de respecter les règles, la sécurité de l'information et la cybersécurité sont devenues des sujets transverses qui touchent les organisations, leurs collaborateurs et plus largement l'ensemble des citoyens. Il est donc nécessaire de favoriser une culture de la sécurité avec pour maîtres mots : 1. simplicité – chacun peut et doit protéger la société – ; 2. pragmatisme – le dispositif doit s'adapter aux contraintes et au niveau de maturité des collaborateurs – ; et 3. agilité – la sécurité est un concept en mouvement permanent.

Notes

1. La mobilisation des professionnels de la gestion d'actifs face aux risques de cybersécurité est au cœur du groupe de travail cybersécurité de l'Association française de la gestion financière (AFG) que préside Arnaud Tanguy. Ce groupe de travail contribue notamment à promouvoir la sensibilisation des collaborateurs des sociétés de gestion aux problématiques de protection de l'information.

2. https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

3. Phishing *ou « hameçonnage » : technique visant à envoyer un message électronique en se faisant passer pour un émetteur de confiance afin de provoquer un vol ou une fuite d'informations ou de perpétrer des actes de piratage électronique.*

4. Ou social engineering *: pratique visant à obtenir par manipulation mentale une information confidentielle.*

5. https://www.appannie.com/fr/insights/market-data/app-annie-2017-retrospective/

6. https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/enjeux-cyber.html

7. http://www.afg.asso.fr/categorie-de-document/etudes-et-analyses/cybersecurite-fr/

La protection des données personnelles éthique vs technologie

Michael Nguyen

Head of Management and Control, Scor

La protection des données personnelles n'est pas une nécessité mais un devoir pour les assureurs. En effet, compte tenu de la sensibilité des données traitées, une cyberattaque n'impacterait pas uniquement l'entreprise, mais potentiellement la vie privée de tous ses clients. Comment quantifier le préjudice pour une personne dont l'employeur découvrirait qu'elle a une maladie grave ou pour celui dont le conjoint apprendrait qu'il n'est pas le bénéficiaire de son assurance vie ? Protéger les données personnelles n'est pas une chose aisée, surtout dans le secteur de l'assurance, qui dispose de données historiques très importantes. Nous proposons dans cet article une démarche pour relever ce défi, en identifiant, grâce à l'ensemble des métiers où se trouvent ces données, qui les utilise avec quelle finalité, puis en sécurisant les accès à celles-ci et en utilisant des moyens tels que le chiffrement ou l'anonymisation pour réduire les impacts en cas de cyberattaque. Au-delà de ces mesures, la technologie permet également aujourd'hui d'envisager des moyens proactifs de profilage des employés et de potentiels futurs hackers pour identifier les risques de cybercrime, grâce à des algorithmes d'analyse prédictive. Mais l'usage de ces moyens nouveaux ouvre un débat éthique : est-il envisageable de faire confiance à une intelligence artificielle (IA) pour juger le comportement humain au nom de la protection des entreprises ?

À l'heure de la connexion permanente (téléphones portables, bracelets d'activités, télévisions et enceintes connectées, etc.), les données personnelles sont récoltées, échangées en permanence sans même que nous en soyons véritablement conscients. Analysée, traitée, revendue : la donnée fait aujourd'hui l'objet d'un véritable marché, estimé à plus de 203 milliards d'euros d'après IDC, avec une croissance annuelle estimée de 11,7 % d'ici à 2020 (1).

En parallèle de l'explosion de ce marché, les fraudes à la carte bleue, l'usurpation d'identité, les e-mails frauduleux, le chantage et les escroqueries sur Internet ne cessent de croître. L'année dernière, le nombre d'individus ayant été confrontés à la cybercriminalité a augmenté de 44 %, pour atteindre 978 millions de personnes dans le monde. Norton estime le coût de la cybercriminalité à 146,3 milliards d'euros en 2017 (2). Les assureurs pourraient profiter de ces évolutions pour trouver un relais de croissance et proposer

des services nouveaux comme la protection des entreprises (le marché de la cyberassurance est estimé à 10 milliards de dollars en 2020 d'après PwC) et des particuliers face aux cybercrimes. Toutefois, pour être crédibles, les assureurs devront démontrer qu'ils sont eux-mêmes bien armés face aux cyberattaques et qu'ils maîtrisent au mieux le cycle de leurs données. Ils doivent donc aujourd'hui faire face à un double enjeu : acquérir davantage de données pour évaluer de façon plus précise et plus profitable le risque client, mais aussi se défendre de façon efficace contre les cyberattaques.

Nous étudierons pourquoi et comment les entreprises peuvent mieux protéger leurs données personnelles. Puis nous nous interrogerons sur les possibilités nouvelles de protection que nous offre l'IA, tout en abordant les questions éthiques que cela soulève.

Pourquoi et comment protéger les données personnelles ?

Les entreprises, et plus particulièrement les assureurs, doivent protéger les données personnelles en leur possession pour trois raisons principales : se protéger des cyberattaques et des risques financier et de réputation associés, se conformer aux régulations et assurer un devoir envers leurs clients, qui leur confient parfois des données très sensibles comme les données médicales. Aujourd'hui, ce n'est plus un choix mais une obligation, et les autorités de régulation à travers le monde renforcent les directives et les règlements en vigueur pour s'assurer que les entreprises respectent ce devoir. En Europe, le nouveau règlement général sur la protection des données (RGPD), qui sera appliqué en Europe en mai 2018, impose un certain nombre d'obligations concernant la sécurité des traitements et le droit des personnes. En résumé, une entreprise devra prouver qu'elle connaît tous les traitements qu'elle opère sur les données personnelles, que ceux-ci sont licites et consentis par les personnes à qui les données appartiennent et que les moyens de sécurité adéquats sont en place, comme par exemple le chiffrement des données ou l'anonymisation, pour éviter toute violation de données. De plus, le RGPD renforce le droit des personnes, qui peuvent exiger auprès des entreprises d'accéder, de rectifier et d'effacer toutes les informations qu'elles possèdent sur elles. Selon EY, seul un tiers des entreprises mondiales répondraient aux exigences du RGPD en mai 2018 (3).

Que faire pour s'adapter à l'évolution du paysage réglementaire et mieux protéger les données personnelles face aux cyberattaques ? Nous proposons une démarche en deux étapes : identifier où se trouvent les données personnelles et qui s'en sert dans l'entreprise, puis en sécuriser l'accès et le contenu.

Où se trouvent les données et quels en sont les usages ?

Où se trouvent les données personnelles et qui dans l'entreprise en a quel(s) usage(s) ? Cette question peut sembler triviale, et, pourtant, dans le métier séculaire qu'est celui de l'assurance, avec des archives nombreuses, des opérations de fusions-acquisitions multiples, un historique de traitements importants, la maîtrise et la connaissance des données acquises ou produites ne sont pas forcément toujours les meilleures. Or, il est essentiel de bien identifier où se trouve la donnée afin de mieux la protéger.

Pour ce faire, un chantier transversal à l'entreprise doit être piloté avec pour point de départ l'établissement d'un registre des traitements utilisant des données personnelles. Il s'agit de définir avec tous les métiers (vie, non vie, investissement, ressources humaines…) quels sont les traitements qu'ils mènent et qui utilisent les données personnelles.

Exemple de traitement : les RH mènent, au nom de la « direction de gestion du personnel France », un traitement intitulé « paie » qui utilise les données personnelles « nom, prénom, adresse de l'employé, IBAN » et qui a pour finalité le paiement du salaire des employés.

Une fois l'ensemble des traitements de données personnelles collectés dans un registre, il convient d'identifier tous les flux de données sous-jacents. Dans l'exemple cité plus haut, la paie peut être lancée à partir d'une base de données « employés » qui se trouve dans un fichier Excel, la campagne d'envoi des fiches de paie traitée par une application informatique, et le résultat final matérialisé sous format papier. Toutes les étapes techniques qui sous-tendent ce traitement de données personnelles doivent être sécurisées pour garantir une protection de bout en bout.

Sécuriser les traitements des données personnelles

Après avoir identifié tous les traitements, il faut déterminer qui accède à quelle donnée et avec quels droits (lecture, écriture…), mettre en place un moyen de surveillance et de suivi des modifications de ces données et, enfin, protéger leur contenu au moyen du chiffrement ou de l'anonymisation.

Qui accède à quelle donnée et avec quel(s) droit(s) ?

Le contrôle des accès est indispensable dans la protection des données. En effet, la plupart des cas de violation de données interviennent lorsqu'un individu souhaite pénétrer dans un système d'information en subtilisant les accès d'une personne autorisée. Il convient donc de mettre en place pour chacun des systèmes contenant des données personnelles, que ce soit une application, une base de données ou un dossier partagé sur le réseau, un système de profils et de ségrégation des vues pour que seules les personnes habilitées puissent y accéder avec des droits particuliers prédéterminés.

Exemple : seuls les collaborateurs de l'équipe de gestion des sinistres automobiles peuvent accéder aux dossiers contenant des informations médicales sur les dommages corporels aggravés.

Une fois ces règles d'accès mises en place, il faut aussi établir un processus de revue des droits des utilisateurs de façon périodique. En effet, cela éviterait qu'un employé qui a quitté l'entreprise ait encore accès aux applications ou, par exemple, qu'un DRH qui a changé de département pour aller dans une direction métier puisse encore accéder aux dossiers des salaires de l'ensemble des employés. La revue périodique des droits est aussi importante que le principe de droits d'accès lui-même et est souvent négligée.

Enfin, au-delà de la revue des droits des utilisateurs, l'entreprise doit également revoir régulièrement les droits des administrateurs informatiques qui créent et attribuent les accès aux employés. En effet, le but ultime recherché par les hackers est souvent de pouvoir se faire passer pour un administrateur, dont les droits étendus permettent virtuellement de pouvoir tout faire dans un système, d'où la nécessité de protéger davantage ces accès particuliers.

Après avoir mis en place un système de droits d'accès avec des profils, ainsi qu'un processus de revue régulière de ceux-ci, la deuxième barrière de défense consiste à implémenter un système de surveillance et de suivi des données.

Surveillance et suivi des données

Un système de surveillance accru capable de remonter des alertes automatiquement en cas d'opérations douteuses (un vol de données, par exemple) est nécessaire à tout système d'information. Pour cela, deux moyens techniques sont à considérer. Une première solution consiste à mettre en place un système qui permet de conserver l'historique de toutes les opérations (*log management*), pour recueillir des indices en cas d'incident et remonter à la source en identifiant les criminels. Une deuxième mesure consiste à utiliser un système de gestion d'événements, tel un *Security Operations Center* (SOC). Le SOC est une sorte de tour de contrôle qui surveille tout ce qui se passe au niveau du système d'information et qui déclenche des alertes selon des règles prédéfinies, comme, par exemple, une sortie massive de données en très peu de temps, cas typique d'une cyberattaque.

Il sert de système de défense pour détecter et contenir une attaque, mais permet aussi d'enquêter a posteriori, en identifiant et en analysant les traces et le mode opératoire des hackers.

Au-delà de ces deux premières barrières de défense, le contrôle des accès et le système de surveillance, il existe un troisième moyen que les entreprises peuvent mettre en œuvre pour minimiser l'impact d'une attaque : la modification des données grâce à des procédés de chiffrement, d'anonymisation ou de « pseudonymisation ».

◆ Réduire le risque : chiffrement, anonymisation et « pseudonymisation»

Le chiffrement est un procédé de cryptographie grâce auquel on peut rendre la compréhension d'une donnée impossible à toute personne qui ne possède pas la clé de déchiffrement. Ainsi, même volé, un document chiffré ne peut être lu et a par conséquent peu de valeur. Le chiffrement peut s'opérer à différents niveaux : stockage de la donnée, système d'exploitation, la base de données, application ou protocoles de transport de la donnée. Une entreprise devra déterminer la manière de chiffrer ses données selon ses moyens, la sensibilité de ses données et l'évaluation du risque encouru.

Une autre technique consiste à anonymiser ses données personnelles, c'est-à-dire à modifier le contenu ou la structure des données afin de rendre très difficile, voire impossible, l'identification de la personne à qui appartiennent ces données.

Exemple : si un set de données comprend les informations « prénom, nom, date de naissance, lieu de naissance », par exemple « Emmanuel, Macron, 21/12/1977, Amiens », il est possible d'identifier la personne à laquelle se réfèrent ces informations. En revanche, si nous procédons à une anonymisation à l'issue de laquelle il ne nous reste que les informations « prénom » et « lieu de naissance », il est impossible d'identifier une personne physique unique, car il y a beaucoup d'Emmanuel nés à Amiens.

Enfin, une dernière technique consiste à « pseudonymiser », c'est-à-dire à effectuer une anonymisation réversible : au lieu de supprimer les informations qui permettent d'identifier une personne, comme c'est le cas avec l'anonymisation, les informations tronquées sont substituées par un « pseudonyme ». Dans l'exemple plus haut, nous aurions un set de données avec « Emmanuel, Amiens, 2335381 », le dernier numéro représentant un pseudonyme qui n'a aucun sens pour ceux qui ne possèdent pas la clé de correspondance mais grâce auquel il est possible de retrouver les informations initiales. D'où le fait que la pseudonymisation est un processus réversible, contrairement à l'anonymisation, qui est irréversible. Anonymisation ou pseudonymisation permettent, en cas de cyberattaque, d'amoindrir l'impact potentiel d'une subtilisation de données.

Nous venons de voir comment protéger les données grâce à trois barrières de défense : contrôle des accès, surveillance du système d'information et moyen de modification de la donnée pour augmenter sa confidentialité. Or, il se développe aujourd'hui des techniques nouvelles fondées sur l'IA qui pourraient sécuriser davantage les données de l'entreprise.

IA : la sécurisation préventive à l'épreuve de l'éthique

Tous les moyens que nous venons de voir constituent des mesures réactives mises en place afin de se protéger contre de futures cyberattaques. Et, pour aller plus loin, il serait possible aujourd'hui d'identifier de façon préventive les futures attaques. En effet, à l'heure du *big data*, les entreprises sont capables de déterminer de façon prédictive les intérêts et les comportements de futurs clients. La plupart des sites Internet actuels enregistrent, grâce à des *cookies* ou à des *trackers*, ce que fait le visiteur, le temps qu'il passe à lire un article, les liens sur lesquels il clique, puis le suivent de site en site en corrélant ces informations avec toutes les autres sources qu'ils posséderaient sur lui : histo-

rique des vidéos vues, recherches sur Internet, etc. Grâce à ces informations, il est désormais possible de parvenir à un profilage des personnes, ce que pratiquent les entreprises pour mieux cibler et vendre leurs services. Le profilage peut également avoir d'autres fins. Facebook a dévoilé dernièrement la mise en place d'une IA capable de détecter des risques de suicide avant que le passage à l'acte n'ait effectivement lieu, grâce à l'analyse des publications de la personne sur son site. De la même façon, il serait possible de détecter un début de conduite cybercriminelle par l'analyse détaillée des comportements caractéristiques d'un hacker avant de passer à l'acte. La menace n'étant pas uniquement externe, une entreprise pourrait également décider de mettre en place ce système de détection proactive parmi ses employés. Il pourrait exister des comportements identifiables caractéristiques d'un vol de donnée ou d'une malversation interne qu'une entreprise serait à même de détecter afin de les neutraliser.

Cette analyse proactive pose toutefois une question éthique. Pouvons-nous donner le droit à un algorithme de décider si oui ou non une personne représente un risque ? Plus encore, acceptons-nous que cette menace potentielle soit fondée sur une analyse impossible à suivre pour l'esprit humain ?

En effet, pour juger une personne, nous procédons à l'analyse de faits, de preuves et de conditions que l'homme est capable d'appréhender. L'être humain est en mesure de faire des comparaisons et d'arriver à une conclusion logique comme celle-ci : cette personne vient d'un milieu défavorisé, vit dans un quartier où le taux de criminalité est élevé, dans une famille monoparentale avec un parent souvent absent, elle a déjà commis un crime mineur d'excès de vitesse, possède un niveau d'études peu élevé, elle est sans emploi… Cette personne sera a priori plus encline à commettre un vol à l'étalage, par exemple, qu'une personne venant d'un milieu bourgeois qui a un revenu élevé et un casier judiciaire vierge. En revanche, dans le monde du *big data*, l'analyse de millions de données provenant de millions de criminels peut permettre d'identifier des corrélations avérées mais difficilement logiques pour un esprit humain, comme, par exemple, trouver une relation entre les personnes qui ont acheté ce type particulier de voiture et qui aiment une catégorie spécifique de films d'action, et la probabilité élevée de commettre un type particulier de crime. Bien entendu, l'analyse de l'IA ne concerne pas uniquement deux catégories mais des millions, sur un échantillon très large d'individus, ce qui lui permet de trouver des corrélations qu'aucun être humain n'est capable de déterminer. Le résultat : une analyse avec une probabilité certainement plus proche de la réalité, mais que personne ne comprendra.

Pourrions-nous accepter de juger un employé pour un crime qu'il n'a pas encore commis et que peut-être il ne commettra jamais simplement parce qu'une IA a conclu que cette personne représentait un risque ? Quand bien même les raisons de mettre en place ce système d'analyse proactive paraîtraient compréhensibles, quels abus est-il possible de commettre au nom des intérêts d'une entreprise ? Au-delà du risque de cyberattaque, un employeur pourrait, par exemple, trouver une raison valable pour surveiller ses employés et déterminer qu'un de ses collaborateurs va bientôt avoir une maladie sévère en corrélant son âge, l'historique de ses arrêts maladie, l'évolution de son appétit à la cantine, la fréquence à laquelle il tousse ou va aux toilettes, etc. Et de conclure que cela constituerait un risque pour son entreprise de lui confier un dossier stratégique qu'il ne pourrait pas suivre, une fois en arrêt maladie.

La protection d'une entreprise peut-elle justifier tous les comportements, dont l'ingérence dans la vie privée ? Où se situent les limites d'une institution en la matière ? Où commence le droit des personnes ?

Face à la menace croissante et à la médiatisation des cyberattaques, les entreprises doivent agir. Cela est d'autant plus vrai lorsqu'il s'agit de données personnelles, car, au-delà de l'impact commercial et du risque de réputation, elles mettent en péril les informations et la vie privée de leurs clients. Il ne s'agit plus d'une nécessité mais d'un devoir, notamment de la part d'entreprises qui possèdent des

données sensibles, comme les assureurs. Aujourd'hui, plusieurs moyens de défense sont possibles, et nous en avons décrit trois dans cet article.

L'évolution du cybercrime et des moyens technologiques va forcer les entreprises à considérer l'IA comme une arme supplémentaire pour leur protection. De cet usage émergera une question d'ordre éthique qu'il convient d'aborder dès à présent, sous peine de laisser se développer des abus favorisés par un flou juridique.

Notes

1. IDC, "Worldwide Semiannual Big Data and Analytics Spending Guide", 2017.

2. Symantec, "2017 : Norton Cyber Security Insights Reports Global Results", 2018.

3. EY, "How Can You Disrupt Risk in An Era of Digital Transformation?", Global Forensic Data Analytics Survey, 2018.

3.

Sécuriser et valoriser les parcours professionnels

Introduction

Pierre-Charles Pradier

Après des interventions chirurgicales sur le Code du travail et l'accès à l'université, le gouvernement se propose de réformer l'apprentissage, la formation professionnelle, et l'assurance chômage avec un seul projet déposé ce printemps par la ministre du Travail. Comme dans les dossiers précédents, cette intervention ciblée et résolue procède d'un diagnostic largement partagé et d'une volonté de remédier efficacement aux risques subis par les travailleurs. Six auteurs nous accompagnent dans la présentation de ce programme de sécurisation des parcours professionnels.

Thierry Vachier rappelle comment la pression de la concurrence et du progrès technologique accélère les transformations de l'emploi : la logique collective passive de défense des emplois n'est plus tenable, et il faut inventer une nouvelle logique, active et préventive qui permet à chacune et chacun de faire prévaloir son projet professionnel dans la durée. À la suite du rapport Davy, le compte personnel d'activité constitue le point de départ d'un compte social unique ; toutefois il semble que les personnes auront besoin d'être accompagnées pour mettre en œuvre ce type de dispositif qui va désormais garantir leurs nouveaux droits, y compris celui au développement professionnel.

Face à ce bel optimisme, ***Jean-Baptiste de Foucauld*** commence par rappeler que la meilleure manière d'assurer la sécurité des parcours, c'est de faire en sorte que l'emploi soit abondant et disponible. En dehors du plein emploi, les techniques de sécurisation des parcours ne peuvent réussir que si elles s'insèrent dans une véritable mobilisation de chacun et de tous, en particulier au profit des plus démunis. L'auteur conclut que le projet de sécurisation suppose un certain esprit de fraternité et ne permet pas d'en faire l'économie.

Face à ces difficultés, ***Hélène Garner*** fait le point sur les politiques publiques de sécurisation : elle rappelle l'inspiration communautaire et l'important travail législatif du quinquennat précédent, qui a conduit à l'instauration des comptes personnel de formation et d'activité. Le problème posé par ces avancées paraît double : d'une part les publics les plus vulnérables sont aussi les plus difficiles à atteindre, il faut concevoir pour eux un accompagnement efficace ; d'autre part, l'individualisation des droits dans ces comptes ne peut s'affranchir d'une régulation qui restreint de facto la liberté des personnes.

Les trois contributeurs suivants nous rappellent que l'État n'est pas le seul acteur des politiques publiques, ce qui permet évidemment de saisir les aspects concrets des transformations en cours.

Ainsi, ***Xavier Bertrand*** présente-t-il les dispositifs spécifiques de la région Hauts-de-France, dans une contribution qui montre la pertinence d'une politique menée au plus près des acteurs de terrain. L'efficacité opérationnelle ne se substitue pas pour autant à la vision d'ensemble : ce texte évoque aussi sans détour les insuffisances des politiques actuelles, et présente des principes pour guider l'action.

Olivier Faron, pour sa part, montre comment la sécurisation des parcours professionnels repose souvent davantage sur une mobilisation bien trouvée des différents dispositifs existants que sur la création ad hoc de nouveaux. C'est dans cet esprit qu'il a engagé la transformation du Conservatoire national des arts et métiers, premier acteur de la formation tout au

long de la vie en France. Un événement symbolique, l'inauguration du nouveau guichet unique par la ministre du Travail en janvier 2018, témoigne de la transformation de l'approche des acteurs de la formation pour proposer une prise en charge globale du projet personnel.

C'est aussi le sujet dont se saisit ***Stéphane Junique*** : celui-ci montre comment les assurés sociaux ont généralement besoin de médiateurs pour activer la nouvelle protection flexible qui leur est proposée. Ces médiateurs doivent concourir à la prévention, c'est-à-dire à l'adoption de comportements responsables par les assurés, mais aussi à la solidarité pour que la personnalisation s'accompagne d'une réduction effective des inégalités. Les acteurs de l'économie solidaire et sociale, avec leur modèle non lucratif, paraissent particulièrement à même d'accompagner le déploiement des nouvelles opportunités de développement professionnel.

D'un monde du savoir à un monde du risque...

Thierry Vachier

Directeur général, Siaci Saint-Honoré

Les transformations permanentes des entreprises sous les coups de boutoir technologiques, économiques et sociologiques génèrent de nouveaux risques de vulnérabilité des salariés. Le traditionnel équilibre « qualité du travail » et « maintien de l'emploi » est pulvérisé au profit d'une nouvelle donne, celle des trajectoires-parcours professionnels et d'employabilité. Dorénavant, c'est la personne en dehors de son statut qu'il convient de sécuriser plutôt que l'emploi. Mais comment concilier la liberté d'entreprendre de l'employeur et la liberté de travailler et de se développer professionnellement pour le salarié ? La France, jusqu'aux ordonnances de 2017, a essentiellement joué la carte de la sécurisation, sans pour autant oser reconnaître dans l'entreprise un droit au développement professionnel du salarié en fonction de son projet personnalisé. Poussé par les jeunes générations (75 % des salariés en 2025 seront nés entre 1980 et 2000 (1)), un autre pacte social reposant sur une relation sociale de donnant-donnant entre l'entreprise et ses salariés émerge doucement : une forme de liberté négociée et la consécration d'un arbitrage personnel tout au long de sa vie, par le biais d'un compte personnalisé de ses droits sociaux, portables, transférables, rechargeables, à abonder. Une évolution inéluctable où les assureurs auront aussi leur mot à dire !

L'analyse de la situation

Le risque de vulnérabilité est un nouveau risque social à gérer ; la vulnérabilité économique individuelle, mais aussi la vulnérabilité collective, c'est-à-dire celle qui est liée aux transformations accélérées du contenu du travail, de son organisation et de son environnement.

Le droit du travail français, et même européen, a d'abord consacré le droit à la sécurité physique à travers la santé. Puis il s'est attaqué au droit de la sécurité par le travail avec la notion de sécurité économique et la continuité du salaire face aux événements de la vie. On peut considérer que la perte d'emploi a plutôt été traitée correctement, tant par le législateur que par les partenaires sociaux. L'édifice de la protection sociale en France n'a pas à rougir de ses réalisations,

qu'il s'agisse des politiques de la santé, de la famille, du logement, du vieillissement, voire de lutte contre la pauvreté. Mais alors pourquoi, depuis plus d'une décennie maintenant, parle-t-on de sécurisation des parcours professionnels ?

Cela est probablement dû à ce sentiment si profond d'imprévisibilité et d'insécurité professionnelle (2) en lien avec l'emploi (destruction/création) et les parcours professionnels actuels ; un sentiment qui prévaut de plus en plus aujourd'hui. Et c'est ce même sentiment qui enracine l'angoisse d'une vulnérabilité économique et sociale croissante, un risque de déclassement potentiel important qui menace tout un chacun. Les raisons de cette situation sont bien connues : le transfert massif de l'activité industrielle des pays développés vers les pays émergents depuis le milieu des années 1990, une phase de délocalisations qui a vu apparaître cette concurrence internationale à bas coûts ; une société de plus en plus vieillissante, et donc moins encline à prendre des risques ; la digitalisation de tous les secteurs d'activité, et la fracture numérique qu'elle peut supposer ; sans oublier, bien sûr, le renforcement de l'automatisation des tâches routinières et l'impact de l'intelligence artificielle à venir sur tous les pans de l'économie.

La conséquence de ces évolutions cumulées est sans appel : plus de 35 % des hommes et un peu moins de 30 % des femmes interrogés dans une enquête Insee (3) affirment que le chômage et la précarité sont la première de leurs préoccupations sur les huit énoncées (4).

Dans le même temps, la société du savoir couplée au développement exponentiel d'Internet et de ses dérivés fait toujours plus appel « aux travailleurs du savoir » décrits comme étant de plus en plus talentueux. Les transformations des entreprises et des organisations sont permanentes pour s'adapter au monde nouveau. Mais la plasticité qu'elle engendre, l'agilité qu'elle commande, la vitesse qu'elle exige… provoquent des transformations souvent importantes, tant au niveau du corps social qu'au niveau des individus. Cela peut donner le vertige car tout le monde n'est pas entrepreneur ! Pourtant, cette peur n'est pas un phénomène nouveau dans l'histoire. Souvenons-nous des *Luddites* anglais des années 1811-1812 – surnommés les « briseurs de machines » – qui voyaient déjà, dans ces machines industrielles qu'étaient les métiers à tisser, la forme d'un nouveau risque social. La nouveauté aujourd'hui, c'est que ce risque exige dorénavant le courage d'y apporter d'autres formes de réponses !

Notre pacte social est en fait en pleine évolution. Il passe progressivement d'une situation « qualité du travail bien fait contre stabilité de l'emploi » à celle du « développement des compétences contre employabilité ». Bien évidemment, aucun des acteurs sociaux, à quelque niveau qu'il se situe, n'est resté les bras croisés face à ce nouveau risque de vulnérabilité économique et sociale des individus. Les mutations en cours vont :

- du « diplôme sésame à vie » à un renouvellement des métiers, et donc, à l'actualisation des connaissances et à l'acquisition de compétences nouvelles ;

- d'une carrière linéaire et stable à des trajectoires professionnelles aujourd'hui, et donc à des parcours de professionnalisation de salariés nomades. Ces trajectoires seront gérées de façon qualitative et individualisée. Dans ce cadre-là, la formation ne sera plus la gestion sociale du salarié mais la gestion d'un risque social ;

- d'une analyse des besoins en emplois et compétences à condition d'être acteur, pour chaque salarié, de son développement professionnel.

En bref, nous passons d'une logique collective (passive) d'assurances sociales à une logique préventive (active).

Le problème à traiter est clair. Il s'agit de sécuriser les personnes plus que les emplois en vue de les aider à traverser les phases de transition qui rythment une trajectoire professionnelle. Mais alors, comment proposer des trajectoires individualisées d'évolution

professionnelle avec des ressources de formation nouvelles, c'est-à-dire avec des garanties équilibrées en contrepartie des nouveaux risques liés aux mutations du travail ?

Toute une série de questions se pose derrière ce nouvel équilibre à bâtir. Elles sont délicates, difficiles à mettre en œuvre... mais il est impératif d'y répondre.

- Peut-on, veut-on et sait-on créer un état professionnel qui garantirait la continuité d'une trajectoire plutôt que la stabilité d'un emploi ?

- Peut-on accepter, face à une approche qui serait de stricte employabilité, de laisser croître la responsabilité des salariés envers leur formation et leur emploi, sans moyen réel d'y faire face ?

- Peut-on, veut-on et sait-on développer un autre modèle social avec un statut de la transition professionnelle et s'engager dans une autre relation d'emploi où chacun est entrepreneur de sa vie professionnelle ?

Quelles solutions

La réaction du droit français face à cette vague de fond

Comme souvent, l'inspiration vient d'ailleurs. La Commission européenne insiste depuis 2007 sur la flexicurité avec la réussite indispensable des transitions professionnelles « en aidant les travailleurs à s'adapter et à accepter le changement ». La réponse française, jusqu'aux récentes ordonnances de 2017, a plutôt été d'accentuer la composante « sécurité » en préférant parler de « sécurisation des parcours professionnels ». La multiplicité des intervenants et des systèmes en la matière a nourri la culture tellement française de « production de dispositifs » juridiques ou autres. Il est cependant incontestable d'affirmer que les textes ont progressivement fait avancer le débat et l'état des lieux en permettant de disposer d'outils à la fois importants et fragmentés : l'accord national interprofessionnel (ANI) du 5 décembre 2003, suivi de la loi du 7 janvier 2014 ; l'ANI du 7 janvier 2009 (formation tout au long de la vie professionnelle, sécurisation, parcours professionnels) puis la loi du 24 novembre 2009 sur le fonds paritaire de sécurisation ; la loi du 8 août 2016 sur la modernisation du dialogue social et la sécurisation des parcours professionnels.

Ces textes ont certes permis un encadrement juridique de dispositifs parcellaires et complexes en accélérant leur convergence, mais le système qui les inspire demeure encore trop dual, réservant la partie « flex » à l'entreprise dans la sphère économique, et la partie « sécurisation » au salarié dans la sphère sociale.

Plus que jamais, c'est une logique de services permanent aux personnes qu'il faudrait adopter, privilégiant ainsi le conseil professionnel et non la prescription dans des dispositifs.

Une boussole pour se repérer dans le monde particulier de la formation

La Commission européenne prône depuis 2007 le « *lifelong learning* », c'est-à-dire la formation tout au long de la vie, du préscolaire jusqu'à la retraite, en y intégrant l'éducation, la formation formelle, informelle, non formelle. L'objectif est qu'un individu poursuive une formation dans une perspective personnelle, physique, sociale en vue d'un emploi, et donc de dépasser son propre statut.

Pour rappel, la flexisécurité ou flexicurité nous arrive des Pays-Bas et a trouvé son épanouissement au Danemark où, pour faire simple, la relative facilité de recruter et de licencier librement pour l'employeur a été compensée par la garantie de revenus et de moyens de reconversion en cas de perte d'emploi ; et ce, grâce à une décentralisation importante des décisions et à un dialogue social de qualité. C'est ici que l'on retrouve l'inspiration des récentes

ordonnances de 2017 en France ! Mais avant tout, comment se repérer dans ce monde si particulier qu'est la formation ?

La professionnalisation est une nouvelle façon d'aborder la formation dans les entreprises avec un nouveau format pédagogique. Elle est devenue un concept juridique avec, entre autres, le droit individuel à la formation (DIF) qui se traduit, dans les faits, par une personnalisation du parcours de formation avec l'alternance juxtaposée ou intégrée, et l'ingénierie de la compétence comme source de la sécurisation des parcours (traçabilité des compétences/certification).

De son côté, le parcours professionnel se traduit par l'instauration de passerelles entre situations de vie, continuation de l'expérience, des droits, des statuts, et il alterne des périodes d'emploi, de formation, d'accompagnement, d'évaluation... Les types de parcours sont variés entre ceux dits d'insertion (employabilité), de gestion des mobilités subies, de professionnalisation (prévention des mutations et déqualification), de gestion de la mobilité professionnelle choisie (promotion professionnelle et réorientation). Les Canadiens, à juste titre, traitent plutôt de transition que de parcours, c'est-à-dire du passage du statut d'emploi, de la position d'emploi aux transitions en emploi, autour de l'emploi, hors emploi. Il est important d'établir une cartographie des mobilités au cours des trajectoires comme par exemple celles concernant l'école/emploi, le chômage/emploi, le non-emploi/emploi, l'emploi/emploi, l'emploi/famille, l'emploi/retraite…

En matière de sécurisation, le concept est emprunté aux relations internationales. Elle traduit la façon dont certains objets, thèmes ou entités sont perçus comme des enjeux de sécurité en requérant des mesures spécifiques, et parfois extraordinaires, afin de les défendre. Cela fait essentiellement référence à des questions d'aléas. Une question demeure pourtant : pourquoi utiliser un tel terme qui illustre, dans l'inconscient collectif, une idée d'immobilisme plutôt qu'une idée d'agilité ? La sécurisation consiste en fait à faciliter la transition entre les différentes situations qu'un individu peut rencontrer dans son existence, à reconnaître le parcours comme une catégorie juridique à part entière, c'est-à-dire avec des garanties collectives pour les individus en contrepartie équilibrée des investissements personnels qui leur sont demandés pour s'adapter. Le but est bien de créer des passerelles entre travail, assurance chômage, solidarité, assistance. Et faire que les individus puissent s'investir complètement dans le développement de leur projet professionnel avec une relative tranquillité d'esprit, au moins apparente, sur des sujets à craindre.

En conclusion, la sécurisation des parcours professionnels revient à améliorer l'employabilité individuelle tout au long de la vie. Mais celle-ci ne s'apprécie pas seulement au sens de l'Organisation internationale du travail (OIT) comme « l'aptitude de chacun à trouver et conserver un emploi, à progresser au travail et à s'adapter au changement tout au long de la vie professionnelle ». Elle n'est pas uniquement liée au niveau de compétences de l'intéressé. Bien au contraire, elle est cette aptitude à mobiliser tout son potentiel personnel, toutes ses capacités, et tient donc compte de sa situation personnelle.

Ce processus fonctionne-t-il pour autant ? Difficile à dire. Mais une chose paraît sûre : être efficace suppose de passer d'une logique de compétences à une logique de capacités (employabilité). Raisonner en termes de capacités signifie que la personne est une fin en soi et que sont prises en compte toutes les dimensions de l'homme au travail (performance, compétences, justice, respect, sécurité) et donc son développement professionnel. C'est aussi reconnaître sa capacité de choisir et de réaliser ses propres choix.

Alors, disons-le, en parlant de sécurisation des parcours professionnels, il ne s'agit, ni plus ni moins, d'entreprendre une réforme de la relation sociale autour de la liberté humaine et une modification de la répartition des risques induits entre les trois acteurs que sont les individus, l'entreprise et l'appareil étatico-social qui gère la formation professionnelle.

Une société de projets, gage de liberté d'entreprendre et de relation de donnant-donnant ?

La réforme de la relation sociale s'ordonne autour d'une autre relation d'emploi avec l'émergence de l'initiative personnelle où chacun est prioritairement l'entrepreneur de sa vie professionnelle.

La formation ne serait donc pas un bien en soi, avec promotion automatique, mais l'ouverture du champ des possibles : liberté professionnelle, possibilité de prise en main de son propre destin, capacité d'exprimer ses préférences professionnelles. Serait-ce alors un droit qui serait reconnu et lié à la personne elle-même, et non à son statut ? Non, pas encore ! Le pas n'est pas tout à fait franchi, le législateur ayant essentiellement développé le concept juridique de la liberté professionnelle, ou plutôt de la liberté contractuelle, comme l'aménagement de la formation, les modalités de départ en formation, l'exécution de la formation (portabilité du DIF par exemple). Dans une perpétuelle relation de subordination juridique, et non dans l'esprit de l'article 14 de la Charte des droits fondamentaux de l'Union européenne.

Vers la modification de la répartition des risques

Nous avons vu que la primauté revient à la personne dans une société de projet où elle se doit de définir son ambition personnelle et professionnelle sur le long terme et de trouver le juste rapport entre son temps de travail et ses autres temps de vie. Les trajectoires professionnelles deviennent alors la traduction des évolutions professionnelles et sociales actuelles. Nous le savons bien, les conditions de travail peuvent être source de vulnérabilité professionnelle. C'est donc une tout autre gouvernance qu'il faudrait promouvoir, une gouvernance qui ouvrirait des espaces de discussion aux projets personnels. L'engagement collectif ne se présupposant plus, il importe de construire une relation de donnant-donnant entre le salarié et l'entreprise, une relation où le salarié disposerait d'un support collectif annuel lui conférant une liberté d'agir et de choisir entre des options telles que le temps, la rémunération et la formation en fonction de ses priorités (santé, famille, relations, éducation/formation, évolution professionnelle, logement, retraite, finances, etc.) liées à son capital personnel. Le salarié réaliserait alors ses choix grâce aux contributions (autofinancées ?) de l'entreprise sous forme de « *fringe benefits* », ou plus précisément de « *soft benefits* » adaptés. En contrepartie l'entreprise sera, elle, en droit d'exiger du salarié un engagement professionnel de qualité et entreprenant. Il s'agit donc davantage d'une liberté négociée, une sorte de droit à décision partagée.

Quant à l'État, et d'une manière plus générale les structures et les systèmes de formation, il leur incombera, dans cette société de projet, d'organiser la protection des populations dites à risque, comme les jeunes peu qualifiés, les seniors, les licenciés, les chômeurs de longue durée. Et le mouvement a bel et bien commencé avec l'instauration d'un droit à l'orientation et d'un droit à la formation qualifiante différée pour les jeunes de seize à vingt-cinq ans en l'absence de qualification à la sortie du système scolaire, avec une prise en charge financière. Le rapport Davy demande d'ailleurs un rééquilibrage de la relation entre l'État et l'entreprise, qui pourrait aussi être une forme de donnant-donnant prônant, en contrepartie d'une participation de l'État, l'obligation pour les entreprises d'assumer les conséquences sociales individuelles d'un licenciement ou de devenir des centres d'apprentissage au niveau régional, cet échelon d'intervention étant estimé comme le plus pertinent.

Quid des assureurs ? Comment formaliser le risque à assurer ?

Une fois encore, le rapport Davy évoque une solution intégrée qui favoriserait l'essor de cette société de projet et de la relation de donnant-donnant qui en découlerait. Le compte universel de droits sociaux

permettrait à chaque personne de gérer ses droits sociaux (épargne retraite, droit au chômage, droit à la formation, sécurité sociale, compte épargne temps...) avec une reconnaissance de leur portabilité, de leur transférabilité, voire de leur possibilité d'être rechargés. Ce serait un excellent moyen personnalisé de sécuriser son propre parcours professionnel depuis l'école jusqu'à la retraite, et d'inciter à la responsabilité de chacun dans l'organisation de ses propres passerelles entre le compte épargne temps (CET, arbitrage personnel temps/argent), le compte personnel de formation (CPF, arbitrage personnel temps/argent/formation) et le compte personnel d'activité [5] (CPA).

Des abondements de l'entreprise, voire de l'État, pourraient alors être mis en place en fonction de conditions précises. Mais pour cela, il faudra bien en assurer la gestion par un tiers patenté. Son rôle sera d'assurer la portabilité et la transférabilité d'un tel compte personnel. Mais on pourrait très bien imaginer que son rôle puisse aller au-delà de la gestion. Pourquoi ne pas alors imaginer un système de bonification ou de plancher selon la qualité du salarié, son potentiel d'apprentissage, sa capacité à s'adapter ?

Alors à nos crayons optiques, à nos planches à dessin virtuelles pour concevoir, en 3D s'il vous plaît, un tel système novateur auquel les nouvelles générations nous conduiront sans faillir.

Notes

1. Deloitte et cadreemploi.fr*, Étude « Qualité de vie au travail. Et le bonheur ? », 2015.*

2. François Davy, « Sécuriser les parcours professionnels par la création d'un compte social universel », rapport remis au ministre du Travail, de l'Emploi et de la Santé, 2012.

3. Statistisques du site insee.fr*, « Préoccupations des Français selon le sexe en 2016 ».*

4. Les huit préoccupations proposées sont « chômage, précarité de l'emploi », « terrorisme, attentats », « pauvreté », « santé », « délinquance », « racisme, discrimination », « environnement », « sécurité routière ».

5. Créé en 2016, il regroupe les droits issus de trois comptes : le compte personnel de formation (CPF), le compte de prévention de la pénibilité et le compte d'engagement.

Sécurisation des parcours des exigences pour réussir

Jean-Baptiste de Foucauld

Ancien commissaire au Plan

Coordinateur du Pacte civique

Ancien président de Solidarités nouvelles face au chômage

La sécurisation des parcours, pour être effective, ne peut être que la composante particulière d'une démarche globale. Elle doit respecter plusieurs conditions : éviter un désengagement de la collectivité vis-à-vis du plein-emploi et un report massif des responsabilités du chômage sur les personnes ; organiser parallèlement des formes appropriées de mobilisation collective pour l'emploi ; élever le niveau de la responsabilité sociale des entreprises ; organiser un accompagnement des personnes d'autant plus dense que le temps de recherche d'emploi s'allonge ; relier parcours professionnels et parcours de vie ; expérimenter des formes de sécurisation différentes de celle des droits de tirage sociaux. Et enfin, sécuriser en priorité les parcours des personnes qui en ont le plus besoin, et qui sont souvent, en fait, privées de parcours.

L'accent mis aujourd'hui sur la sécurisation des parcours et sur les techniques qui permettent de la mettre en œuvre, comporte des risques qui ne sont pas assez mis en valeur dans le débat actuel. C'est sur ce point que je voudrais insister, car ils font apparaître par symétrie, les conditions de réussite de cette approche. Celle-ci doit être systémique et non pas ponctuelle. Ce ne peut être une simple méthode qu'il suffirait de placer au sein d'un système lui-même profondément déséquilibré. La sécurisation des parcours, pour être effective, ne peut être que la composante particulière d'une démarche globale. Or, elle est le plus souvent présentée comme un remède autosuffisant. Comme un processus d'adaptation à un marché du travail déséquilibré, pesant plus particulièrement sur les personnes en difficulté ou pouvant l'être, auxquelles il convient de donner des moyens de réagir efficacement. Il n'est pas contestable que ceci soit nécessaire. Mais ce n'est pas pour autant suffisant. Or la tentation est grande de faire de la sécurisation des parcours la nouvelle recette magique de la lutte contre le chômage, venant après d'autres (la baisse du coût du travail, les 35 heures, etc.), se suffisant à elle-même. Il n'en est rien. Pour réussir, la sécurisation des parcours doit respecter les conditions suivantes.

Conditions pour une sécurisation effective

Éviter un désengagement de la collectivité vis-à-vis du plein emploi

La meilleure manière d'assurer la sécurité des parcours, c'est de faire en sorte que l'emploi soit abondant et disponible ; si cette condition est remplie, les ruptures, aussi pénibles soient-elles, peuvent être assez vite réparées et on peut alors parler de parcours vers l'emploi. Au contraire, dans une situation de

chômage de masse, et de chômage de longue durée importante, la notion de parcours n'a plus le même sens : le parcours risque de s'avérer parking, sinon parcage. Certes, un parcours bien accompagné pourra aboutir à créer de l'emploi, par exemple grâce à la création d'activités, ou à l'occupation de postes de travail qui n'arrivaient pas à être pourvus, avec des effets multiplicateurs réels ; mais ces aspects positifs seront marginaux si la situation du marché du travail est par trop déséquilibrée : le développement des compétences n'assure pas ipso facto l'employabilité et l'emploi. En un mot, si un parcours bien mené peut faire émerger de l'emploi, c'est en premier lieu l'existence des emplois qui facilite la réussite des parcours. Il faut regarder la relation entre parcours et emploi des deux côtés à la fois, et constater qu'ils ne sont pas symétriques. C'est plus l'existence des emplois qui permet les parcours que l'organisation des parcours qui fait émerger l'emploi.

Il ne faut donc pas abandonner l'objectif du plein-emploi, et même du plein-emploi de qualité, cela contre vents et marées. Or, l'accent mis sur la sécurisation des parcours peut s'accompagner d'un déplacement des préoccupations, d'une résignation de fait devant le chômage et la précarité, devenir une pure stratégie adaptative, si l'on n'y prend pas garde. De même, les possibilités d'action plus grandes données aux personnes peuvent justifier un moindre sens des devoirs de la collectivité vis-à-vis de ces mêmes personnes, la mise en jeu de leurs capacités se substituant à l'action collective contre le chômage. Ce processus d'individualisation risque ainsi d'être lié à une démobilisation de la collectivité et à une moindre implication de celle-ci, les responsabilités du chômage étant alors, en toute bonne conscience, reportées excessivement sur les personnes.

Organiser parallèlement des formes appropriées de mobilisation collective pour l'emploi

Il est essentiel de ne pas tomber dans ces tentations ou ces contradictions, car elles sont de nature à faire échouer le processus de sécurisation des parcours : non seulement les techniques de sécurisation des parcours ne justifient pas une implication moindre de la collectivité vis-à-vis de l'emploi, mais elles ne peuvent réussir que si elles s'insèrent dans une véritable mobilisation collective des forces sociales organisées et des citoyens en faveur d'un plein-emploi de qualité. Telle est la leçon que nous donnent les pays d'Europe du Nord qui ont réussi à mettre en œuvre la fameuse flexicurité : elle s'insère dans une capacité de compromis économique et social en faveur d'un plein-emploi de qualité qui assure un haut niveau d'emploi.

De manière générale, l'économie de marché suppose une attention particulière de tous les acteurs aux questions d'emploi, qui ne va pas de soi et doit être organisée, car il est par nature difficile de concilier la liberté d'entreprendre, la liberté du travail, et le pleinemploi.

Le risque est donc que notre pays importe la recette de la sécurisation sans se préoccuper de son contexte et des conditions qui lui permettent de donner toute son efficacité. Le fait est que notre pays n'a jamais su jusqu'ici organiser une véritable mobilisation collective durable face au chômage et ne dispose ni d'un compromis État/marché, ni d'un compromis capital/travail qui sont nécessaires au bon fonctionnement d'une économie sociale de marché ou d'une social-démocratie. La sécurisation des parcours ne peut suppléer ces conditions de base, ce qui crée un risque de nouvelle déception et de maintien de la défiance. Il est donc essentiel de bien articuler les responsabilités collectives et les responsabilités individuelles.

Il est significatif que, parmi les deux formules possibles de sécurisation, celle des droits de tirage sociaux, inspirée des travaux d'Alain Supiot, et celle du contrat d'activité, formulée en son temps par Jean Boissonnat, la première, plus individualiste, soit seule mise en avant, la seconde, engageant plus la collectivité, n'ayant pas même été expérimentée ; de même, l'expérimentation « Territoires zéro chômeur de longue durée » ne semble pas être considérée comme une forme de sécurisation, alors qu'elle l'est

profondément et reprend d'ailleurs des intuitions du rapport Boissonnat. Un rééquilibrage de notre approche en faveur d'une vision plus systémique et globale s'impose donc.

Élever le niveau de la responsabilité sociale des entreprises

La sécurisation des parcours se joue pour une grande part dans l'entreprise. Or, les rapports de force au sein de l'économie de marché se sont profondément modifiés. Pendant les Trente Glorieuses, les managers et les salariés (« le monde du travail ») se sont trouvés en position de force par rapport aux consommateurs, auxquels ils infligeaient des taux d'inflation élevés, et par rapport aux actionnaires et obligataires, qui étaient traités, sinon à la marge, du moins en priorité de second rang. La situation est aujourd'hui complètement retournée : le monde du travail est pris en tenaille entre les consommateurs et les actionnaires. Il subit une double pression : d'une part, les consommateurs réclament des prix bas et des produits de qualité, et font jouer la concurrence ; d'autre part, les actionnaires, exigeants, veulent des taux de rentabilité élevés et ont tendance à mettre les dirigeants de leur côté afin que la gestion des entreprises soit principalement orientée vers l'objectif de rentabilité, les structures de production à faible rentabilité étant éliminées.

La sécurisation des parcours, pour être effective et mériter son nom, doit donc être accompagnée d'actions qui corrigent peu à peu cette situation : émergence d'une consommation socialement responsable (qui reste à inventer), développement de l'investissement socialement responsable (ISR) et de l'actionnariat participatif des salariés, pénalisation fiscale des taux de rentabilité exagérés, management moins soumis aux diktats des financiers et plus ouvert sur les besoins des diverses parties prenantes. Dans les entreprises, l'option pour la flexibilité interne chaque fois qu'elle est possible plutôt que pour la flexibilité externe, des plans de formation élevant le niveau de qualification des salariés fragiles ou menacés, l'implication dans l'apprentissage, la capacité à recruter des personnes issues des quartiers en difficulté ou connaissant un chômage de longue durée constituent des conditions nécessaires à la réussite pour une sécurisation des parcours équilibrée. Les recherches en cours sur le régime juridique de l'entreprise, son rapport avec l'intérêt général, vont également dans ce sens.

Une sécurisation des parcours effective suppose un accompagnement des personnes

Ce besoin doit être reconnu, qu'il s'agisse d'orientation, de reconversion ou de recherche d'emploi, particulièrement lorsque celle-ci s'allonge dans le temps et que le découragement gagne. L'accompagnement doit être d'autant plus intense que les difficultés de la personne sont grandes. Il ne peut pas être fait par l'employeur, monopolisé par l'organisation du travail, mais par un tiers dit tiers de confiance, qui peut être une équipe [1], diverses méthodes étant envisageables. Cet accompagnement a, d'une manière ou d'une autre, un coût qu'il ne faut pas se dissimuler et qui doit être prévu et pris en charge, ce qui n'est que très imparfaitement le cas, car c'est le prix invisible de l'externalisation du chômage que l'on ne veut pas identifier. C'est pourtant le triptyque accompagnement-situation de travail-formation, dont les différents volets doivent pouvoir être mobilisés en permanence tout au long des parcours, qui assure la robustesse de ceux-ci.

Il n'y a pas de bons parcours professionnels sans bons parcours de vie

L'accompagnement n'a d'ailleurs pas pour seul but de mieux réussir la carrière professionnelle ; il doit porter aussi sur les choix de vie, avoir pour but de permettre à chacun de donner le meilleur de lui-même, d'exprimer sa singularité et ses talents dans ce qu'ils ont de plus fécond et parfois d'inattendu, de favoriser une juste autonomie de la personne par rapport aux exigences du système productif. Ce ne doit pas être un stress de plus, mais une manière de

redonner de la distance et du choix. Il s'agit d'inverser la tendance : c'est le parcours de vie qui doit déterminer le parcours professionnel, et non l'inverse ; à tout le moins un équilibre doit s'instaurer entre ces deux priorités, le but étant que peu à peu chacun développe son activité dans ce qui est sa vocation, là où il a le plus de chance d'apporter les fruits de son unicité. Il en résulte deux conséquences :

– d'une part, les différentes formes de temps choisi, sans précarité ni pénalité, doivent être disponibles pour les personnes aux différents stades de leur parcours, car l'élaboration de ces choix de vie suppose du temps, des tâtonnements, des expériences ; cela suppose donc des efforts d'organisation importants pour permettre ces choix, et aussi un changement culturel dans le rapport au travail [Foucauld, 2010] ;

– d'autre part, une définition large des formations disponibles au sein des parcours, afin qu'elles correspondent aux choix et aux recherches des personnes et pas seulement aux contraintes professionnelles, permettant en outre de dépasser les éventuels déficiences de l'éducation initiale.

Il serait utile d'expérimenter le contrat d'activité

Proposé par le rapport Boissonnat [1995], ce dispositif aurait consisté à rattacher les personnes à une structure unique qui leur permette d'occuper diverses positions d'activité (salariat à temps plein ou partiel, autoentrepreneur, formation, recherche d'emploi) sans avoir à changer de statut, ce qui assure une présence collective derrière les personnes, et devrait s'avérer plus simple, plus souple et en définitive plus protecteur que le système des droits de tirage sociaux où la charge de l'activation des différents dispositifs existants repose presque exclusivement sur la personne. Certaines formules de portage salarial proches de l'économie sociale et solidaire ne sont pas loin de cela. Une expérience sur une échelle plus vaste, dans l'esprit de celle des territoires zéro chômeur de longue durée mériterait d'être tentée, afin d'enrichir les voies d'accès à la sécurisation des parcours.

Il faut sécuriser en priorité les parcours des personnes qui en ont le plus besoin, et qui sont de fait privées de parcours

Les différentes formules de sécurisation actuellement envisagées risquent de laisser de côté les personnes écartées depuis longtemps du marché du travail et qui ont épuisé leurs droits. Faut-il rappeler qu'il y a en France environ 500 000 bénéficiaires de l'allocation spécifique de solidarité et 1,8 million d'allocataires du revenu de solidarité active (RSA) socle, dont environ 200 000 entrent et sortent chaque année. Il ne s'agit pas là de « sécuriser » un parcours, mais tout simplement d'en offrir un, là où il y a une situation qui vaut mieux, certes, que l'absence totale de revenu, mais qui est tout de même fondamentalement insécurisante. Il y a peu de débats sur ces situations, à peine évoquées lors de l'élection présidentielle, alors que l'on devrait se fixer un objectif clair de résorption progressive année par année. Ces personnes ne doivent pas être les oubliées de la sécurisation des parcours, ce qui veut dire qu'un lien doit être fait avec les politiques d'insertion. Ne faut-il pas d'ailleurs que l'ensemble de la société s'impose une sorte de devoir d'insertion ou d'intégration ? Ne pourrait-on demander aux entreprises d'avoir dans leurs effectifs une petite proportion de personnes qui, lors de leur embauche, se trouvaient au chômage de longue durée ou au RSA (2) ? Plusieurs expériences associatives (3) montrent que c'est tout à fait compatible avec une bonne gestion des entreprises et même source de retombées positives.

Pour conclure, la politique de sécurisation des parcours suppose un certain esprit de fraternité (4), conforme à nos valeurs fondamentales ; elle ne permet pas d'en faire l'économie.

Notes

1. Ainsi les bénévoles de Solidarités nouvelles face au chômage accompagnent les chercheurs d'emploi en binôme

et se retrouvent chaque mois dans un groupe de solidarité pour s'aider à aider (voir « Développer un accompagnement personnalisé vers l'emploi sur www.snc.asso.f*).*

2. C'était une des propositions de Catherine Barbaroux et Jean-Baptiste de Foucauld dans leur rapport « Un droit au parcours accompagné vers l'emploi », 1995.

3. Par exemple celle des Clubs régionaux pour l'insertion dans l'industrie (CREPI).

4. Sur ce point, voir les travaux du Pacte civique. www.pacte-civique.org

Bibliographie

FOUCAULD J-B. (de), *L'abondance frugale. Pour une nouvelle solidarité*, Odile Jacob, 2010, p. 213 et suivantes.

BOISSONNAT J., *Le travail dans vingt ans*, rapport du commissariat général du Plan, Odile Jacob, 1995.

Des politiques publiques de sécurisation de l'emploi

Hélène Garner

Directrice du département Travail emploi compétences, France Stratégie

Dans un contexte de mondialisation croissante, à défaut de protéger les emplois, depuis les années 2000, les pouvoirs publics ont privilégié la protection des personnes et la sécurisation des parcours professionnels (SPP), c'est-à-dire la sécurisation des transitions sur le marché du travail, entre deux emplois, entre emploi et chômage, entre études et emploi... Inspirée du droit communautaire, la voie retenue par les pouvoirs publics pour sécuriser les personnes a été de chercher à leur attacher des droits (sociaux, à la formation, à la qualification, à l'accompagnement, à la mobilité), de manière à leur donner les moyens de faire face aux aléas et risques du marché du travail (1). Cela se traduit du point de vue des politiques publiques par une plus grande responsabilisation des individus, censés ainsi devenir des « acteurs de leur parcours », et une plus grande individualisation des dispositifs afin de répondre de façon personnalisée aux besoins des personnes. Mais la sécurisation passe aussi par la construction de cadres collectifs qui garantissent ces droits et permettent leur exercice, sans quoi celle-ci ne profitera qu'aux mieux informés, aux plus éduqués et sera un vecteur d'inégalités accrues entre les actifs. Une tension apparaît alors entre l'autonomie portée par ces dispositifs et leur régulation sociale qui restreint de facto la liberté des personnes.

Les transitions sur le marché du travail augmentent : entre 1980 et 2014, la part des actifs qui, à un an d'intervalle, connaissent une transition professionnelle est passée de 12 % à 17 %. Et cette augmentation est à attribuer presque exclusivement à des épisodes de chômage plus fréquents. Toutes les transitions ne sont pas risquées, et toutes les personnes ne sont pas égales face à ces risques (de chômage, d'obsolescence des compétences, de déqualification, d'éloignement du marché du travail, etc.). Certaines populations y sont plus exposées et cumulent les facteurs de risque (personnes issues de l'immigration, peu diplômées, handicapées, femmes, jeunes, seniors).

Dès lors, il s'agit d'articuler une approche préventive de ces risques en mettant les personnes en capacité – au sens des *capabilities* de Sen –, de ne pas avoir à y faire face (tous les dispositifs dits d'investissement visent cet objectif de réduction de réalisation des risques) avec une approche curative orientée sur le retour en emploi. Au cœur de cette approche

se trouvent des droits individualisés (sociaux, à la formation, à la qualification, à l'accompagnement, à la mobilité) et leur portabilité dans les transitions, mais aussi le cadre collectif et les modalités de régulation dans lesquels ils s'exercent. Si l'expression « sécurisation des parcours professionnels » était initialement plus spécifiquement liée aux politiques de formation, elle a été progressivement étendue à tous les dispositifs individualisés visant le maintien des droits entre deux emplois.

Des droits individualisés au cœur de la SPP

En attachant des droits aux personnes et de moins en moins à l'emploi ou au statut (d'emploi ou de contrat de travail), les pouvoirs publics individualisent des droits qui restent en réalité toujours acquis dans le cadre de l'emploi [Guiomard, 2013]. La première des sécurisations, la sécurisation financière, renvoie à la fois aux allocations d'indemnisation chômage et aux prestations sociales financières et en nature qui ont pour but de maintenir un niveau de vie décent aux personnes. Les évolutions législatives récentes ont ciblé une protection plus individualisée des personnes, que ce soit par la création des droits rechargeables à l'assurance chômage ou les mesures visant à l'extension de la protection sociale – comme l'extension de la complémentaire santé à l'issue du contrat, inscrite dans la loi de 2013 relative à la création de la protection universelle maladie (Puma) –, et par l'obligation pour les plateformes employant des travailleurs indépendants de prendre en charge, à compter de janvier 2018, l'assurance volontaire acquittée par les travailleurs en cas d'accident du travail, ou de leur proposer un contrat collectif.

Les différentes réformes de la formation professionnelle au cours de la dernière décennie traduisent une individualisation croissante de la formation avec à la fois des obligations renforcées de l'employeur en matière d'évaluation et de formation des salariés en place (dont l'entretien professionnel obligatoire tous les deux ans et l'entretien professionnel de bilan tous les six ans), et surtout la création de dispositifs publics personnalisés dont le plus emblématique est le compte personnel de formation (CPF) créé par la loi du 14 juin 2013 relative à la sécurisation de l'emploi. Le CPF est un compte personnel ouvert à tous les actifs et abondé pour les salariés à hauteur de 24 heures maximum par an pour un temps plein, avec un plafond à 150 heures. Il permet ainsi de capitaliser des heures de formation en vue d'obtenir une certification dans une logique de droit d'accès individuel universel à la formation. Dans le texte d'orientation préparé par le gouvernement en vue de la négociation interprofessionnelle qui s'est ouverte en novembre 2017, le CPF apparaît comme le levier majeur de la « liberté professionnelle » des salariés.

La création du compte personnel d'activité (CPA) dans la loi du 17 août 2015 relative au dialogue social et à l'emploi (Titre III. Sécurisation des parcours et retour à l'emploi) marque une étape supplémentaire dans la construction d'une sécurisation des parcours professionnels à la française. Le CPA vise explicitement cet objectif de « rassembler » des droits attachés à la personne : « Afin que chaque personne dispose au 1er janvier 2017 d'un compte personnel d'activité qui rassemble, dès son entrée sur le marché du travail et tout au long de sa vie professionnelle, indépendamment de son statut, les droits sociaux personnels utiles pour sécuriser son parcours professionnel […] ».

Ayant pour objectif selon l'exposé des motifs de la loi du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels « de renforcer l'autonomie et la liberté d'action de son titulaire et de sécuriser son parcours professionnel en levant les freins à la mobilité », le CPA contribue ainsi à la création d'un nouveau droit individuel : le droit à la qualification professionnelle prévoyant de « progresser au cours de sa vie professionnelle d'au moins un niveau en acquérant une qualification correspondant aux besoins de l'économie prévisibles à court ou moyen terme ». Cela se traduit par des abondements complémentaires pour les

publics considérés comme les plus fragiles comme le prévoit la loi travail du 8 août 2016 (ce qui correspond à de nouveaux modes d'alimentation du CPF) :

• les jeunes sortis sans diplôme du système éducatif bénéficient d'un droit au nombre d'heures nécessaires à la réalisation d'une formation qualifiante. Ce droit relève de la compétence des régions ;

• pour les salariés n'ayant pas un niveau de formation correspondant au niveau V du Répertoire national des certifications professionnelles (RNCP), leur CPF sera alimenté de 40 heures par an jusqu'à un plafond de 400 heures ;

• les demandeurs d'emploi peu qualifiés bénéficieront également d'un abondement supplémentaire.

Le plan d'investissement des compétences (PIC) constitue la composante « formation » du grand plan d'investissement (GPI) lancé par le gouvernement pour la période 2018-2022.

• Le PIC représente au total 14,6 milliards d'euros (sur les 57 milliards du GPI). L'essentiel (13,9 milliards) servira à favoriser l'accès à l'emploi pour deux millions de personnes (un million de chômeurs, un million de jeunes décrocheurs) ;

• Sur ces 13,9 milliards d'euros, 7,1 seront dédiés aux demandeurs d'emploi peu qualifiés. Ils financeront prioritairement des formations longues et certifiantes. L'objectif est d'améliorer le taux de retour à l'emploi de ces publics de quinze points (soit 150 000 chômeurs en moins à la fin du quinquennat).

Si la formation des demandeurs d'emploi est depuis 2004 de la responsabilité des régions, les pouvoirs publics nationaux ont depuis 2013 fortement encouragé leur développement, notamment à travers des plans de formation massifs visant des objectifs quantitatifs de demandeurs d'emploi entrés en formation (plan 30 000 en 2013, 100 000 en 2015, et 500 000 en 2016). Malgré ce volontarisme, les dépenses de formation des demandeurs d'emploi ne représentent en France en 2015 que 40 % des dépenses associées aux politiques actives du marché du travail, contre 73 % en Allemagne, et leur montant a reculé entre 2010 et 2015. Si ces plans ont augmenté le taux d'accès à la formation des demandeurs d'emploi, ils n'ont pas permis d'améliorer leur taux de retour à l'emploi durable (2).

Aujourd'hui, l'orientation privilégiée par les pouvoirs publics est de cibler la formation sur les plus fragiles dans une logique d'investissement (*cf.* encadré ci-contre).

La nécessité de cadres collectifs

Par ces dispositifs individualisés, l'État providence évolue et cherche à devenir un État social actif selon les termes du ministre flamand Frank Vandenbroucke. Mais la personnalisation des droits induite par ces évolutions doit s'inscrire dans un cadre collectif de détermination et de garantie de ces droits, principe fondamental de l'État social actif.

Dans le cadre du compte personnel de formation, et plus largement du compte personnel d'activité, comme dans l'ensemble des dispositifs individualisés de type droits rechargeables à l'assurance chômage, les modalités de financement sont assises sur des cotisations mutualisées. Pour le CPF, les entreprises de plus de dix salariés contribuent à hauteur de 0,2 % de leur masse salariale brute. Les entreprises de moins de dix salariés ne versent pas de contribution spécifique mais les salariés de ces entreprises peuvent utiliser leur compte personnel de formation sur les fonds mutualisés. Pour les personnes à la recherche d'un emploi, les heures sont prises en charge par Pôle emploi et les régions. Elles sont refinancées par le Fonds paritaire de sécurisation des parcours professionnels (FPSPP).

Les règles de mobilisation de ces dispositifs sont également encadrées par les partenaires sociaux et/ou le législateur. Ainsi, par exemple, les heures inscrites sur le CPF ne peuvent être mobilisées que pour financer des formations inscrites sur des listes éligibles définies par les partenaires sociaux. Dans la régulation de ces dispositifs le rôle des partenaires sociaux est central (dans le cadre de l'assurance chômage comme dans des instances de gouvernance telles que le Comité interprofessionnel pour l'emploi et la formation – Copanef – ou le Conseil national de l'emploi, de la formation et de l'orientation professionnelles – Cnefop – créés dans la foulée de la loi de 2014 sur la formation professionnelle).

Un des grands risques associés à ces droits et dispositifs individualisés est qu'ils peinent à atteindre les publics fragiles s'ils ne sont pas insérés dans des processus d'accompagnement personnalisés. En effet, le compte, dans sa logique individuelle, risque de renforcer les inégalités entre les personnes car les individus les mieux formés, les mieux informés seront les plus à même de mobiliser leur compte tandis que les plus fragiles risquent de passer à côté des opportunités offertes par le compte. Une manière de contrer cet effet serait d'abonder davantage les comptes des individus les moins qualifiés par exemple (dans une logique de droit à la formation différée) de manière à compenser les inégalités de dotations initiales. Mais les études étrangères montrent que doter financièrement (ou en heures ou en points) les individus les plus éloignés de l'emploi ne suffit pas à ce qu'ils se saisissent de leurs droits [Perez, 2014]. La question de l'accompagnement des individus susceptible de contrer cet effet en offrant aux plus fragiles les moyens de saisir les opportunités offertes par ce compte constitue donc un axe central de la sécurisation des parcours professionnels ; d'abord centré, dans une logique d'activation des politiques de l'emploi, sur les demandeurs d'emploi, l'accompagnement a été récemment étendu à tous les actifs.

Ainsi, en même temps que le compte personnel de formation, les partenaires sociaux ont institué dans l'accord national interprofessionnel (ANI) de 2013 – suivis par le législateur dans la loi du 14 juin 2013 relative à la sécurisation de l'emploi –, le conseil en évolution professionnelle (CEP). Présenté comme un « droit à un accompagnement facilitant la réalisation de choix éclairés et autonomes », il vise à offrir à tous les actifs (y compris les salariés et les non-salariés) un conseil personnalisé, universel et gratuit en orientation professionnelle. Avec le CEP, l'accompagnement n'est plus réservé aux seuls demandeurs d'emploi ou personnes en difficultés mais aussi à ceux en emploi, contribuant à faire de chaque actif un individu en potentielle transition. Si le nombre de bénéficiaires de CEP a doublé entre 2015 et 2016 (pour atteindre 1 541 544 bénéficiaires (3)), il reste un droit encore largement méconnu et à l'offre hétérogène. Et les partenaires sociaux sont invités, dans le cadre de la future réforme de la formation professionnelle à « [...] négocier sur ce que doit être un droit à l'accompagnement au service des actifs et sur ses objectifs comme instrument d'émancipation de l'individu » (4).

La principale difficulté de l'accompagnement réside dans la mise en œuvre effective d'un accueil et d'un conseil personnalisé, tant les situations sont diverses et complexes. Des études qualitatives conduites auprès de salariés licenciés entrés dans le dispositif de contrat de sécurisation professionnelle (CSP) (5) soulignent les écarts existant entre les intentions en matière d'accompagnement personnalisé et la réalité de l'accompagnement reçu par les bénéficiaires. Les auteurs soulignent notamment que les prestations sont fournies de façon fragmentée dans une logique d'empilement, alors que l'accompagnement devrait être pensé de manière globale, articulant les différentes prestations de manière à coconstruire le parcours avec l'individu dans une démarche itérative. Il ressort également de manière marquée que la valeur ajoutée du dispositif repose principalement sur la personnalisation de la relation avec l'adhérent (6). La continuité de l'accompagnement tiendrait avant tout au lien continu, et soutenu, du conseiller avec chaque adhérent qui ne passe pas forcément par des rendez-vous prédéfinis mais par des échanges au fil des besoins, ce qui requiert une certaine liberté dans cette relation.

Entre autonomie et responsabilité

Le discours sur la sécurisation des parcours professionnels (SPP) est presque toujours articulé avec le couple « autonomie/responsabilité ». Les dispositifs de SPP visent à « libérer » les individus en leur donnant les ressources leur permettant de faire face aux aléas du marché du travail, et à en faire des « individus autonomes ». Mais cette autonomie croissante des individus va de pair avec un élargissement de la responsabilité et donc des obligations individuelles, comprises avant tout comme la manifestation de « bonnes » dispositions à participer au marché du travail [Franssen, 2008]. Cette autonomie a donc un coût pour la personne qui devient toujours plus responsable de son parcours professionnel, au fur et à mesure qu'elle est censée être sécurisée, ce qui pose de façon aiguë la question de l'effectivité de ces dispositifs et de leur recours. En outre cette autonomie est encadrée. L'État social actif est en effet un État régulateur, ce qui passe, dans les dispositifs de sécurisation des parcours professionnels, par un fort encadrement des choix de l'individu dans une logique de droits et devoirs (comme par exemple le compte personnel de formation qui finance uniquement des formations inscrites sur des listes éligibles). Cet encadrement repose sur l'idée que les individus ne sont pas toujours en capacité de choisir, de prendre une décision intégrant tous les paramètres relatifs à celle-ci et qu'ils doivent donc être guidés, orientés, encadrés de manière à faire converger intérêt individuel et collectif. Une évaluation expérimentale d'un programme cadre pour l'emploi américain nommé Workforce Investment Act of 1998 semble confirmer cette croyance. Testant trois modalités d'accompagnement à la prise de décision des individus (un mode « libre choix » dans lequel l'individu est laissé libre de l'utilisation de ses droits formation, un mode « directif » dans lequel le choix doit être validé par des agents en charge de leur suivi, et un mode « intermédiaire » reposant sur une forme d'accord entre les individus et leur conseiller avec une marge de négociation), le principal enseignement de cette évaluation est que plus le choix est encadré par des professionnels, plus les revenus des participants augmentent de manière significative.

Pour autant l'encadrement existant dans la mobilisation des droits à formation du CPF est interprété par certains usagers comme la négation d'un compte véritablement personnel, dans la mesure où les titulaires ne sont pas libres d'utiliser leurs droits comme ils le souhaitent (7). Ce qui est en jeu ici, c'est l'articulation entre l'individuel et le collectif : s'il peut paraître légitime, avec des droits abondés par la collectivité ou mutualisés, que les pouvoirs publics (et les partenaires sociaux) encadrent certains choix personnels de manière à en accroître les rendements et les externalités pour l'ensemble de la société, il n'en demeure pas moins que cette option réduit le degré d'initiative laissé aux personnes. Or la perception de cette liberté et des marges de manœuvre dans la mobilisation des droits sera indéniablement un facteur de succès ou un frein dans le développement de ces outils de sécurisation des parcours professionnels.

Notes

1. D'autres modalités de sécurisation font partie du débat, comme la mise en place d'une sécurité sociale professionnelle ou d'un droit personnel à la carrière (cf. *propositions de l'Institut européen du salariat), ou d'un statut de l'actif* (cf. *notamment Supiot [1999]).*

2. Réseau emplois compétences (REC), « Renforcer la capacité des entreprises à recruter », rapport du groupe de travail n° 4, France Stratégie, 2017.

3. Bilan du Conseil national de l'emploi, de la formation et de l'orientation professionnelles (Cnefop), juin 2017.

4. Document d'orientation transmis par le gouvernement aux partenaires sociaux, novembre 2017.

5. Étude Unedic, « Radiographie de la demande et du vécu du contrat de sécurisation professionnelle (CSP), 2014. https://www.unedic.org/sites/default/files/2017-05/demande_et_vecu_du_csp_-_etude_gatard.pdf

6. Credoc/Unedic, « Étude auprès de demandeurs d'emploi sur leurs attentes en matière d'accompagnement au retour à l'emploi durable, 2014. https://www.unedic.org/sites/default/files/2017-04/synthese_credoc_-_unedic_attentes_accompagnement_desdemandeurs_emploi_-_oct_2014_0_0.pdf

7. France Stratégie, « Le compte personnel d'activité, de l'utopie au concret », rapport, 2015.

Bibliographie

FRANSSEN A., « L'État social actif : une reformulation du contrat social ? » *in* Bajoit G. (éd.), *Le contrat social dans un monde globalisé*, n° 33, Academic Press Fribourg, Fribourg, 2008.

GUIOMARD F., « La sécurisation des parcours professionnels. Naissance d'une notion », *Revue de droit du travail*, 2013, p. 616.

PEREZ C., « Regard sur quelques expériences étrangères de "comptes individuels de formation" », *Droit social*, n° 12, décembre 2014, pp. 981-985.

SUPIOT A. (dir.), *Au-delà de l'emploi : transformations du travail et devenir du droit du travail en Europe*, rapport pour la Commission européenne, mars 1999.

Les Hauts-de-France pionniers des politiques de l'emploi

Xavier Bertrand

Président, Région Hauts-de-France

À l'aube de la troisième révolution industrielle, notre économie se transforme de manière exponentielle, au rythme effréné des progrès technologiques. Intelligence artificielle, techno-médecine, impression 3D, big data *et autres méthodes d'apprentissage automatique : cette transformation accélère l'évolution des tâches et des métiers des Français au quotidien. En effet, selon le Conseil d'orientation pour l'emploi, ce phénomène général que l'on peut appeler « automatisation » a le potentiel de transformer la moitié des emplois existants, de manière significative, voire très importante. Quelles politiques de l'emploi devons-nous mettre en place pour répondre à ces nouveaux défis ?*

Ces transformations imposent au moins deux priorités pour notre politique de l'emploi. Premièrement, il est essentiel d'assurer la mise à jour permanente des compétences dans tous les métiers, en particulier dans ceux qui sont le plus exposés à l'automatisation. Deuxièmement, nous devons protéger les individus face à des changements qui peuvent être parfois abrupts, notamment à travers la sécurisation des parcours professionnels.

Mon point de vue sur la sécurisation des parcours professionnels est peut-être trop direct mais il est nécessaire : je pense que notre pays n'est pas aujourd'hui à la hauteur, il n'est pas assez préparé à ces défis gigantesques. Force est de constater que notre politique de formation professionnelle ne remplit pas sa mission, car elle omet largement ceux qu'elle est censée aider en priorité. Pour qu'elle soit véritablement efficace, nous devons respecter un certain nombre de principes, tels que la proximité, la flexibilité ou encore la sécurité. Ce sont ces principes qui guident notre action pour la formation et l'emploi dans les Hauts-de-France.

L'heure des constats : une politique de formation inefficace

La sécurisation des parcours professionnels fait partie intégrante du Code du travail et du droit conventionnel. Pour autant, cette mesure est-elle efficace ? Les chiffres parlent d'eux-mêmes : même en période de croissance, notre taux de chômage stagne à 10 % (contre 4,2 % au Royaume-Uni et 3,6 % en Allemagne), et nous avons

en permanence près de 300 000 offres d'emplois qui ne trouvent pas preneurs. Par exemple, en mars 2017 l'entreprise des services à domicile O2 a lancé une campagne de recrutement de 500 CDI à Lille (1). Un mois plus tard, 460 CDI restaient encore à pourvoir... Pourquoi ? Pas assez de candidats expérimentés, pointe O2.

Ce problème n'est pas nouveau. Nous devons donc effectuer une évaluation globale, rigoureuse et objective des 31 milliards d'euros dépensés (2) chaque année dans la formation professionnelle, afin d'identifier précisément où sont nos lacunes [Dares, 2017]. En effet, le taux moyen d'accès à la formation était de 42,2 % en 2013. Mais cette moyenne cache de grandes disparités : si 32,3 % des ouvriers et 35,4 % des employés ont accès à la formation professionnelle, en revanche ce chiffre passe à 54,6 % pour les ingénieurs et les cadres. De même, seuls 16,6 % des salariés dans les entreprises de 10 à 19 salariés y ont accès, contre 52,9 % pour les entreprises de plus de 2 000 salariés.

Cette situation paradoxale est difficile à comprendre. D'un côté, ceux qui sont le mieux armés pour faire face aux défis de la mondialisation (grandes entreprises et cadres avec un capital humain important) captent la majorité des fonds dédiés à la formation professionnelle. De l'autre, ceux qui sont le moins bien armés et le plus exposés à l'automatisation (petites entreprises, ouvriers, employés) n'en captent qu'une très faible part. De plus, pour cent euros investis par l'État dans la formation, combien d'euros se perdent dans la gestion de celle-ci ? Impossible de le savoir précisément, puisque les chiffres de la Dares ne distinguent pas clairement les dépenses de fonctionnement de celles liées aux rémunérations des formateurs, qui à elles deux absorbaient 61 % du budget de la formation professionnelle, soit près de 20 milliards d'euros. Sur ces 20 milliards d'euros, combien sont dépensés dans des processus administratifs inutiles ? Nous avons le droit et le devoir de savoir : oui à la formation, non à la bureaucratie de la formation. Il s'agit là d'un problème similaire à celui de Pôle Emploi : 33 % des conseillers sont affectés à l'accompagnement de demandeurs d'emploi (contre 51 % au Royaume-Uni), et 32 % aux fonctions support (17 % au Royaume-Uni).

Enfin, la France dispose de plus de 75 000 centres de formation, contre 4 000 en Allemagne. Pourquoi une telle différence ? Pour quelle utilité ? De plus, il semblerait que seuls 8 % de ces centres aient comme activité principale la formation professionnelle. Si cela est avéré, alors quelles sont leurs autres activités ? Ils ne doivent avoir qu'un seul objectif : permettre aux Français de pouvoir toujours trouver un travail de qualité.

Certes, l'État a essayé de rendre ce système moins opaque : la loi sur la réforme de la formation professionnelle (entrée en vigueur le 5 mars 2014) oblige les centres de formation à produire annuellement un bilan pédagogique et financier, afin de rendre compte de leurs véritables activités. Mais pour le moment, la visibilité sur leurs activités réelles et leurs résultats reste minimale. Cela est d'autant moins acceptable que l'on constate que la formation professionnelle reste le meilleur moyen de lutter contre le chômage. En effet, une enquête Ipsos (3), réalisée auprès de mille personnes licenciées pour motif économique en 2009, montre que lorsque les formations sont dispensées, leur efficacité est reconnue : elles ont permis à leurs bénéficiaires de se perfectionner (80 %), de changer de métier (45 %), de se qualifier (47 %) ou de certifier des capacités (34 %). Le développement des compétences professionnelles est la première garantie de sécurité de l'emploi. Donc développer les compétences des individus en lien direct avec les besoins des entreprises est le meilleur moyen de sécuriser les parcours professionnels.

Comment sécuriser les parcours professionnels ?

Quelle doit être la priorité de la sécurisation des parcours professionnels ? D'abord protéger le salarié contre les aléas de la vie et les exigences du marché du travail en évolution permanente.

La priorité ne doit pas être la protection des emplois en soi. Pour cela, nous devons respecter un certain nombre de principes.

Principe n° 1 : le diplôme initial est important mais n'est pas l'alpha et l'omega

Le diplôme initial est important, mais il ne peut servir de sésame à vie. En conséquence, est-il utile de forcer des jeunes à s'enfermer dans des études longues et coûteuses qui les intéressent peu, sous prétexte qu'ils ne vaudraient rien sans diplôme ?

Par ailleurs, l'accélération des évolutions du marché du travail rend d'autant plus importante la formation en continu et la mise à jour des compétences, ainsi que la refonte en amont de la formation initiale.

Cette évolution est une bonne nouvelle. En effet, la France a trop souvent l'obsession des diplômes et des grandes écoles. On confond le fait d'être surdiplômé avec l'employabilité : une personne n'ayant pas de diplôme est tout à fait capable d'être compétente dans son travail. De plus, ce système élitiste qui ne fait confiance qu'aux diplômes est profondément inégalitaire. Il n'est pas acceptable de dire à des jeunes : « À vingt-deux ans, soit vous avez réussi, soit vous avez raté, et c'est pour toujours. »

Principe n° 2 : l'emploi et la formation ne doivent faire qu'un

Ne perdons pas de vue que l'objectif des études et de la formation est de trouver un emploi. Les formations, qu'elles soient initiales, en alternance ou en continu, doivent être le plus professionnalisantes possibles, et donc répondre au mieux aux besoins des futurs employeurs.

Penser l'éducation et la formation en dehors de la question de l'employabilité, c'est les condamner à l'inefficacité. Et penser l'emploi sans penser la formation, c'est courir à l'échec.

Principe n° 3 : la formation doit répondre aux besoins des individus et des entreprises

Certains se demandent si la formation doit être adaptée aux entreprises ou aux individus. Pour moi, c'est un faux problème : la formation doit s'adapter aux individus et aux entreprises. En effet, si la formation n'est pas adaptée à l'individu, elle est inefficace. Et si elle n'est pas adaptée à l'entreprise, elle est inutile.

L'important, afin que les compétences des individus répondent vraiment aux besoins des entreprises, est de lever les multiples obstacles qui les séparent :

– capacité limitée d'accès aux informations nécessaires pour trouver une formation ou un emploi. Une étude de l'Insee de 2014 révèle que seules 53 % des personnes de dix-huit à soixante-quatre ans avaient entendu parler du droit individuel à la formation (DIF) ;

– progression inégale du DIF : en 2008, le taux d'accès au droit individuel à la formation n'était que de 5,5 %, principalement du fait de la complexité de la démarche et de la perte de certaines formations éligibles. Le DIF a été remplacé par le compte personnel de formation (CPF) en 2015. C'est un progrès puisque le CPF est valable tout au long de la vie et est indépendant du contrat du salarié (3,6 millions de CPF ont été ouverts en 2017), mais il va à l'encontre du principe n° 1 (*cf.* ci-dessus) car les formations proposées dépendent du diplôme initial.

– manque de financement pour certaines formations ;

– éloignement géographique de la formation ou de l'emploi ;

– absence de formations pour certains métiers spécifiques ;

– délais d'attente trop longs (supérieurs à six mois) pour les utilisateurs.

Principe n° 4 : oui à la proximité

Une formation « hors-sol » est par définition inadaptée. C'est malheureusement souvent ce qui se passe à Pôle Emploi. Les conseillers font de leur mieux, mais on leur demande de conseiller des chômeurs dans des centaines de métiers différents dont ils ne peuvent avoir l'expertise !

Dans le privé, les conseillers en orientation et formation sont le plus souvent spécialisés. Cela leur permet de donner des conseils vraiment utiles aux chômeurs, par exemple sur les secteurs qui recrutent, ceux où leurs compétences seront le mieux valorisées, ou sur les formations les plus professionnalisantes.

De plus, l'éloignement géographique est très souvent l'une des principales raisons qui bloquent l'accès à un emploi ou à une formation. Aussi, la meilleure garantie de retour à l'emploi est de faire se rencontrer l'offre et la demande d'emploi au niveau local, bassin d'emploi par bassin d'emploi. C'est exactement dans cet esprit que nous avons créé le dispositif Proch'Emploi pour la région des Hauts-de-France. J'y reviendrai.

Principe n° 5 : oui à la flexibilité

Arrêtons les caricatures : la flexibilité dans l'emploi et la formation est nécessaire simplement parce que l'économie est une matière vivante, qui change et fluctue au fil des découvertes technologiques et cycles économiques. Figer l'emploi et la formation, c'est donc les ancrer dans un passé qui devient vite désuet, du fait notamment de l'innovation permanente qui caractérise l'économie contemporaine. Donc, si les emplois évoluent, la formation elle aussi doit évoluer. Est-ce le cas aujourd'hui ? Pas vraiment si l'on observe le nombre d'emplois non pourvus.

La flexibilité, ce n'est donc pas laisser les entreprises réduire leurs effectifs dans des conditions inacceptables. La flexibilité permet surtout à chacun de faire des choix personnels et professionnels, et de changer d'avis s'il le souhaite. Prenons l'exemple des jeunes : aujourd'hui on leur demande de décider de leur avenir à seize ans lorsqu'ils doivent choisir une orientation (L, S, ES, baccalauréat professionnel, etc.). Et s'ils changent d'avis à dix-huit, vingt ou vingt-cinq ? C'est leur droit ! C'est au système éducatif, d'orientation et de formation de s'adapter à leurs choix, pas l'inverse.

Si rien n'est fait, nous n'en finirons jamais avec le chômage des jeunes : avec un jeune sur quatre au chômage en France, c'est toute une génération que l'on sacrifie. C'est un combat que je souhaite mener d'abord à l'échelle de la région des Hauts-de-France. Je veux redonner des perspectives d'avenir à tous les jeunes de la région, pour qu'ils aient envie d'y rester et que la solution ne soit plus de quitter la région ou même le pays ; parce que ce sont eux qui feront vivre la région. Je souhaite même que des jeunes d'autres régions et d'autres pays aient envie de venir chez nous, parce qu'il y aura de l'emploi, parce qu'il fera bon y vivre. Ce combat a commencé il y a deux ans.

Mais si les entreprises veulent de la flexibilité, elles doivent être flexibles elles-mêmes. Il est irréaliste d'attendre d'un employé qu'il soit opérationnel à cent pour cent dès le premier jour de son travail. Partout, dans tous les métiers, et quelle que soit la taille de l'entreprise, il y a une phase d'adaptation. Les entreprises doivent donc faire montre de bonne volonté et être prêtes à former leurs nouvelles recrues. Elles doivent être pleinement associées au processus de formation de leurs employés. Elles ne peuvent pas se plaindre de l'inadéquation des compétences disponibles sur le marché du travail, et parallèlement refuser de s'engager dans la formation de leurs propres employés. Heureusement, la plupart des entreprises que je rencontre dans les Hauts-de-France sont conscientes des enjeux cruciaux de la formation et investissent dans les compétences de leurs employés, comme Toyota ou Bridgestone, par exemple.

Principe n° 6 : oui à la sécurité

La flexibilité et la sécurité de l'emploi ne sont pas aussi antinomiques qu'on le dit. Elles sont toutes deux nécessaires, et il serait aberrant de les opposer

l'une à l'autre. En effet, beaucoup pensent (à tort) que les entreprises veulent simplement de la flexibilité et les individus simplement de la sécurité.

Mais la flexibilité est aussi dans l'intérêt des employés : un marché du travail trop rigide pousse chacun à se raccrocher le plus possible à son emploi, même si on ne l'aime plus.

De même, la sécurité de l'emploi est également dans l'intérêt des employeurs, car elle permet à leurs employés d'être moins sujets au stress, et donc plus efficaces. En effet, une étude Cegos [2016] montre qu'un quart des salariés ont déjà connu un épisode de *burn-out* ou de dépression. Cela impacte directement le monde de l'entreprise, à travers une augmentation de l'absentéisme et une baisse de la productivité.

Expérimentations en région des Hauts-de-France

Le gouvernement présentera son projet de loi sur la réforme de la formation professionnelle au printemps 2018. Je souhaite que les principes cités ci-dessus soient pris en compte. Mais il n'est pas possible d'en rester aux seuls mots : j'ai donc cherché à appliquer certains de ces principes à l'échelle de la région que j'ai le plaisir de présider, les Hauts-de-France.

Tout d'abord, nous avons créé Proch'Emploi. Avec Proch'Emploi, nous cherchons à rapprocher les demandeurs d'emplois des employeurs qui ont du mal à recruter, notamment en utilisant une compétence importante de la région : la formation. Ce dispositif s'appuie sur un réseau de vingt-et-une plateformes territoriales destinées aux entreprises, implantées dans chacun des bassins d'emploi de la région. Cela crée des « circuits courts » d'embauche – permettant ainsi aux demandeurs d'emploi de rencontrer localement des entreprises et des conseillers en orientation –, et développe également les réseaux locaux d'entrepreneurs. À la date du 12 février 2018, Proch'Emploi a permis à environ 7 300 personnes de trouver, soit un emploi (84 %), soit une formation (16 %).

Dans la même logique, nous avons lancé les dispositifs Pass Emploi (pour les entreprises) et Pass formation (pour les demandeurs d'emplois).

Le Pass Emploi permet aux entreprises de recevoir des aides financières pour former de futurs collaborateurs, à une condition : qu'elles s'engagent à les recruter. Cela crée donc un lien direct entre la formation et l'emploi. C'est le dispositif qu'a récemment choisi Bonduelle, numéro un français de la transformation de légumes pour embaucher cent cinquante nouveaux saisonniers par an pendant cinq ans. Comme l'explique Thierry Baptiste, responsable des ressources humaines de Bonduelle : « D'ici 2020 […] notre niveau d'exigence – déjà très élevé – va encore augmenter. […] Notre volonté est donc de former en amont nos futurs salariés, pour qu'ils acquièrent un socle d'aptitudes indispensable à leur recrutement. »

Le chèque Pass Formation, de son côté, soutient les projets individuels de formation des demandeurs d'emploi. Les projets visés incluent la formation pour des métiers prioritaires, la création ou la reprise d'entreprise, et la reprise d'activité après licenciement économique. Cela permet au demandeur d'emploi d'accéder à une formation qui lui apporte, soit des compétences, soit une certification professionnelle. L'une des premières à avoir bénéficié du Pass Formation est Aurélie Groubatch, trente-deux ans. Elle avait démissionné de son poste d'agent de sécurité pour devenir boulangère : « Avec l'aide d'un conseiller (Proch'Emploi), j'ai monté un dossier. Peu de temps après, j'apprenais la bonne nouvelle : je pouvais bénéficier d'une aide régionale de 4 000 euros, le chèque Pass Formation. Si tout va bien, d'ici quelques mois, j'obtiendrai mon contrat d'aptitude professionnelle (CAP). Et je pourrai ouvrir ma boulangerie ! »

Enfin, en janvier 2017 nous avons lancé un dispositif pour minimiser l'obstacle que constitue l'éloignement géographique dans le retour à l'emploi : « En route pour l'emploi ». Avec ce dispositif, la

région met à disposition une voiture, pour deux euros par jour, à tout demandeur d'emploi qui a retrouvé un emploi mais n'a pas de moyen de locomotion pour se rendre à son travail. Au vu du succès rencontré, nous avons étendu ce dispositif aux jeunes en alternance ou en apprentissage. Plus récemment, l'entreprise Toyota, qui emploie 3 600 personnes dans la région, s'est associée au dispositif en mettant à disposition dix Yaris, produites dans les Hauts-de-France.

Avec ces différentes initiatives, nous souhaitons prouver que si la sécurisation des parcours professionnels dépend en partie de l'initiative individuelle, elle découle également de la capacité et de la volonté de tous les acteurs du travail – nationaux et locaux – de réduire les multiples obstacles qui barrent la route de l'emploi.

Notes

1. lavoixdunord.fr*, « Les 460 offres d'emploi en CDI du leader du service à domicile ne trouvent pas preneurs » par Patrick Seghi, 10 avril 2017.*

2. formation-ideale.com*, « La formation professionnelle en chiffres : les données à effet retard ».*

*3. Enquête Ipsos citée dans un article de Philippe Dole (*cf. *bibliographie).*

Bibliographie

Baromètre de l'observatoire Cegos, « Climat social et qualité de vie au travail », 18e édition, 15 novembre 2016.

communication-agefice.fr

Conseil d'orientation pour l'emploi, « Automatisation, numérisation et emploi. Tome 1. Les impacts sur le volume, la structure et la localisation de l'emploi », janvier 2017.

Direction de l'animation de la recherche, des études et des statistiques (Dares), « La dépense nationale pour la formation professionnelle continue et l'apprentissage en 2014 », *Dares Résultats*, n° 041, juin 2017.

Dole Ph., « Sécurisation des parcours professionnels : regards croisés », *Pour*, n° 207, vol. 4, 2010.

Gossiaux S. ; Pommier P., « La formation des adultes. Un accès plus fréquent pour les jeunes, les salariés des grandes entreprises et les plus diplômés », *Insee Première*, n° 1468, octobre 2013.

Institut national de la statistique et des études économiques, « L'accès des adultes à la formation en 2012 », *Insee Résultats*, n° 160, octobre 2014.

Jakubowicz L., « Macron et formation professionnelle : tout savoir sur la réforme », *journaldunet.com*, 3 janvier 2018.

journaldunet.com, « CPF : le compte personnel de formation », 22 janvier 2018.

maformation.fr, « Qu'est-ce qu'un OPCA et à quoi sert-il ? », 20 août 2015.

Picut G., « La formation continue, une priorité pour sécuriser les parcours professionnels », *lemonde.fr*, 13 octobre 2017.

service-public-pro.fr, « Prise en charge des formations des travailleurs indépendants », 2 juillet 2017.

Totet N., « Le premier bilan positif de Proch'emploi », *courrier-picard.fr*, 14 juillet 2017.

Le Cnam et la sécurisation des parcours professionnels

Olivier Faron

Administrateur général, Conservatoire national des arts et métiers (Cnam)

La notion de sécurisation des parcours professionnels constitue une réponse au besoin croissant des actifs d'être accompagnés lors de transitions professionnelles devenues plus fréquentes, voire inévitables en raison des mutations économiques. Mettre opérationnellement en œuvre la sécurisation des parcours professionnels convoque une pluralité de registres allant de l'ingénierie socio-pédagogique à la définition d'un cadre juridique idoine, en passant par la gestion des compétences au sein des opérateurs mobilisés. Cette sécurisation des parcours professionnels a vocation à s'incarner dans le cadre d'une articulation bien trouvée des offres de services existantes qui devront parfois être complétées. La contribution potentielle des organismes de formation à la sécurisation des parcours professionnels est cruciale. L'exemple du Cnam en atteste : mise en place de guichets uniques AIOA (accueil, information, orientation et accompagnement), modularisation des parcours d'accès à la certification, définition d'une fonction accompagnement, etc.

Mutations économiques et mobilités professionnelles

Au regard des mutations économiques qui affectent les emplois et les compétences, les carrières professionnelles sont d'ores et déjà moins linéaires qu'elles ne l'étaient auparavant. Cette tendance devrait s'accroître au cours des années à venir, notamment au regard des impacts potentiels sur l'emploi de la numérisation, de l'automatisation et de la robotisation…

Ce contexte de mobilité professionnelle accrue permettra à certains actifs dotés de compétences rares ou très demandées de se saisir des opportunités professionnelles qui se présentent. En effet, la nécessaire adaptation aux besoins du marché du travail constituera probablement, pour celles et ceux que l'on nomme les « *insiders* », une occasion d'affirmer une singularité et des talents. Pour d'autres actifs, pour ceux ne maîtrisant pas les savoirs de base ou bien pour les moins qualifiés, potentiels « *outsiders* » d'un marché du travail toujours plus polarisé, la mobilité professionnelle imposée par ces évolutions est synonyme d'entrée dans une zone de risque de chômage et de précarité : une forme de trappe.

La notion de sécurisation des parcours professionnels a émergé dans cette situation où l'augmentation de la mobilité professionnelle impose aux personnes d'acquérir de nouvelles compétences pour se maintenir en emploi. La sécurisation des parcours professionnels

se trouve, en réalité, convoquée dans une diversité de cas :

• transition emploi-emploi et transition emploi-chômage ;

• mobilité subie et mobilité choisie ;

• mobilité interne à l'entreprise et mobilité externe à l'entreprise ;

• en prévention ou en réaction, au moment de la mutation économique.

Le véritable enjeu consiste à mettre en œuvre opérationnellement cette sécurisation des parcours professionnels (SPP) et donc à l'incarner. C'est à cette tâche que s'attellent les services du Cnam. Signe des temps, le service Information orientation du centre Cnam de Paris a récemment été réorganisé. Inauguré fin janvier 2018 par la ministre en charge du Travail, Muriel Pénicaud, il se nomme désormais « La fabrique des compétences ».

Conditions de succès de la mise en œuvre de la SPP

À l'aune de l'expérience du Conservatoire national des arts et métiers, il est possible d'identifier quatre conditions de succès de la sécurisation des parcours professionnels :

• accompagner la mutation de l'offre de services en matière d'accueil, d'information, d'orientation et d'accompagnement (AIOA) afin d'être en capacité de formaliser des parcours professionnels répondant aux situations de mobilités professionnelles vécues par les personnes ;

• identifier les différentes composantes afin d'individualiser les parcours et d'industrialiser cette individualisation, selon un modèle économique soutenable pour les financeurs et pour les opérateurs ;

• définir une mission d'accompagnateur des parcours, ce qui implique de préciser cette notion un peu « valise » d'accompagnement ainsi que la posture et les compétences de l'accompagnateur ;

• adapter le cadre juridique afin de rendre possible, dans le cadre du droit commun, la prise en charge en termes d'actes métiers et de financement des différentes étapes d'un parcours.

Il en ressort que la sécurisation des parcours professionnels repose sur un mixte, une forme d'alchimie, convoquant :

• une ingénierie socio-pédagogique ;

• une gestion des compétences spécifique mobilisée par les opérateurs sollicités ;

• un cadre juridique adapté.

Former, ce n'est pas sécuriser les parcours professionnels à tout moment et sans le savoir...

Il existe dans la palette des dispositifs issus des politiques publiques ou paritaires d'emploi et de formation professionnelle, un certain nombre d'outils mobilisables dans le cadre de démarches de sécurisation des parcours professionnels. Nous en citons ci-après quelques exemples et cela, sans prétendre à l'exhaustivité mais en nous positionnant sur différentes étapes de la chaîne :

• orientation professionnelle et ingénierie de parcours ;

• modularisation des parcours de développement des compétences ;

• traçabilité des démarches de définition de projet et d'acquisition des compétences.

Au titre des outils d'appui à l'orientation professionnelle et à l'ingénierie de parcours, figurent le bilan

de compétences ainsi que le conseil en évolution professionnelle. Il s'agit de deux outils, créés à des moments relativement distants dans le temps (1991 et 2014). Leur rôle est repensé aujourd'hui, au regard de leurs complémentarités tant en termes de finalités que de formats pédagogiques.

La modularisation de certifications professionnelles dans le cadre de leur découpage en blocs de compétences constitue la condition de l'ingénierie de parcours modulaires permettant, dans un contexte de mobilité professionnelle, aux actifs tant d'aller chercher les compétences manquantes que de valider progressivement la totalité d'une certification. Cette modularisation des parcours est susceptible de s'articuler intelligemment avec le dispositif de validation des acquis de l'expérience (VAE) initié au début des années 2000 par Vincent Merle qui fut, par la suite, titulaire de la chaire « emploi, travail et acquisitions professionnelles » du Cnam. Le dispositif de VAE constitue un élément totalement précurseur dans la palette des outils opérationnels mobilisables au service de l'ingénierie des parcours professionnels.

Le passeport orientation emploi compétences, objet qui revient de manière récurrente dans l'agenda social depuis une quinzaine d'années (mais peine à s'incarner en un outil homogène et approprié par tous), constitue un puissant catalyseur potentiel de la sécurisation des parcours professionnels. Il permet aux actifs de garder la trace de leurs démarches en matière d'orientation professionnelle et d'identifier les diverses compétences qu'ils ont acquises tant à la faveur de situations de travail que de formations formelles. Cet outil connaît depuis la loi du 5 mars 2014 une consécration juridique sous la dénomination de passeport d'orientation, de formation et de compétences (*cf.* article L. 6323-8 du Code du travail).

À quelques exceptions, au titre desquelles on peut mentionner le contrat de sécurisation professionnelle (CSP), la sécurisation des parcours professionnels repose davantage sur une mobilisation bien trouvée des différents dispositifs existants que sur la création ad hoc d'outils clé en mains. Pour autant, on ne contribue pas à sécuriser les parcours professionnels à tout moment et sans le savoir, à la manière d'un Monsieur Jourdain qui découvrait avec émerveillement la pratique de la prose…

En réalité, la sécurisation des parcours professionnels implique :

- ex ante, de procéder à une analyse « carencée » de l'offre de services mobilisable, à l'aune de quelques parcours types (par exemple, parcours de mobilité subie, parcours de mobilité choisie, parcours d'insertion, etc.) pour combler les manques éventuels au sein de l'offre de services ;

- in itinere, de mettre en musique les différentes briques de l'offre de services et de coordonner la mobilisation des acteurs de back office afin que la complexité inhérente à l'ingénierie d'un parcours soit la plus transparente possible pour l'utilisateur final ;

- ex post, d'assurer un suivi de la mise en œuvre du parcours et si possible, d'en évaluer les effets sur le maintien dans l'emploi, le retour à l'emploi, l'entretien du lien social, etc.

Histoire d'une lente émergence dans le corpus juridique

Pour être effectivement praticable, la sécurisation des parcours professionnels doit faire l'objet d'une inscription dans le corpus juridique qu'il s'agisse du droit conventionnel (accords signés par les partenaires sociaux) ou du droit régalien (lois et règlements). Il s'agit là de la condition de la prise en charge financière des différentes étapes d'un parcours et de la reconnaissance statutaire des publics visés. Sont mentionnés ci-après quelques éléments historiques de cette saisie par le droit de la notion de sécurisation des parcours professionnels.

Au niveau des branches professionnelles, la sécurisation des parcours professionnels constitue un objet du dialogue social dont les partenaires sociaux se sont saisis, depuis un certain temps, dans le cadre des

commissions paritaires nationales de l'emploi (CPNE) et des conseils d'administration paritaires des organismes paritaires collecteurs agréés (OPCA).

• Les premiers certificats de qualification professionnelle (CQP) et certificats de qualification professionnelle interbranches (CQPI) ont vu le jour, à l'initiative des partenaires sociaux, à la fin des années 1980. Ils ont souvent été créés à destination de secteurs professionnels accueillant une forte proportion de salariés peu ou pas qualifiés. Dans un contexte de mutations économiques impactant fortement les emplois, pour faciliter les transitions professionnelles, il convenait de signaler les compétences détenues par ces salariés dans le cadre de la validation d'un CQP ou d'un CQPI qui constituait un gage de maintien dans l'emploi ou de retour à l'emploi ;

• L'identification par les partenaires sociaux de priorités de formation auxquelles est affectée une partie des fonds mutualisés gérés par les organismes paritaires collecteurs agréés (OPCA) a permis (dans bon nombre de cas) d'anticiper ou d'accompagner des mobilités professionnelles de salariés dans certains secteurs économiques ;

• Les démarches de VAE collectives constituent, quant à elles, un outil d'accompagnement particulièrement approprié en cas d'évolutions professionnelles permettant de passer d'un métier d'origine menacé à un métier cible émergent ou en développement.

Au niveau interprofessionnel, la sécurisation des parcours professionnels a connu une lente reconnaissance à la faveur d'accords nationaux interprofessionnels (ANI) et de lois :

• La notion de « parcours » apparaît dès le titre 1er « Faciliter l'entrée dans l'entreprise et améliorer l'entrée en emploi » de l'ANI du 11 janvier 2008 consacré à la modernisation du marché du travail ;

• La loi du 24 novembre 2009, qui entérine la création d'un fonds paritaire de sécurisation des parcours professionnels (FPSPP) fait entrer la notion de sécurisation des parcours professionnels dans la partie législative du Code du travail ;

• Certaines dispositions de la loi du 8 août 2016 viennent, quant à elles, préciser la contribution potentielle de la formation à la sécurisation des parcours professionnels, notamment à travers la notion dite de « forfait parcours » (cf. articles L. 6352-2 et L. 6332-14 du Code du travail).

La fabrique de la sécurisation des parcours professionnels au Cnam

« Il enseigne à tous et partout », telle est la devise ambitieuse et à visée universaliste du Cnam. Cela implique une grande vigilance en matière de sécurisation des parcours des actifs qui viennent se former au Cnam, notamment lorsque cette démarche intervient à un moment où ils peuvent éventuellement être en difficulté sur le marché du travail.

À l'aune de la mission de formation professionnelle tout au long de la vie du Cnam, les leviers de la sécurisation des parcours professionnels que nous mobilisons renvoient à trois principaux registres :

• prise en charge de la complexité du back office pour apporter des réponses opérationnelles aux actifs dans le cadre de la mise en place d'un « guichet unique ». Avant tout engagement dans un parcours de formation, le Cnam propose des moments d'échange et de réflexion (entretiens individuels) aux futurs auditeurs qui prennent la forme d'un conseil individuel en formation. Ce conseil permet à l'auditeur d'analyser ses motivations d'entrée en formation, de clarifier les objectifs visés, d'envisager des possibilités de financement et de faire le choix de formation le plus pertinent par rapport à son projet personnel et professionnel. Ce conseil est dispensé au niveau national par des personnels dédiés (conseillers formation,

conseillers d'orientation) et par des enseignants. Cette prestation gratuite est proposée durant des temps forts d'inscription mais aussi tout au long de l'année. En termes d'évolution de cette prestation de conseil, un travail est actuellement conduit pour envisager des modalités à distance des entretiens-conseils à destination d'auditeurs éloignés territorialement. Par ailleurs, depuis plus d'un an, le Cnam organise des temps d'échange renforcé avec les financeurs de la formation pour répondre au mieux aux nouvelles contraintes réglementaires et accompagner les publics dans la construction de leur parcours de formation. Dans cet esprit, la « fabrique des compétences », située au centre Cnam de Paris (CCP), est assimilable à une forme de guichet unique d'AIOA ;

• prise en compte de l'approche chronologique du parcours pour formaliser des réponses formatives adaptées aux contraintes de temps des actifs. Le Cnam, notamment au regard de sa pratique de cours du soir (formations hors temps de travail), a fortement investi sur des pratiques permettant la validation progressive de la totalité d'une certification. Dans la droite ligne de la réforme de la formation de 2014, la direction nationale des formations du Conservatoire s'est engagée dans un travail de grande ampleur consistant à identifier des blocs de compétences au sein des certifications professionnelles délivrées. Par ailleurs, dans le cadre d'une démarche menée avec l'ensemble des centres Cnam en région, a été formalisée, dès 2013, une charte de l'accompagnement VAE. Cette méthodologie d'accompagnement VAE est fondée sur des phases individuelles et collectives et se situe au cœur de la qualité du service rendu par le Cnam à un candidat à la VAE. De nombreuses campagnes de communication visent à promouvoir cette voie d'accès aux certifications professionnelles représentée par la VAE.

• contribution à la définition d'une fonction d'accompagnement ne faisant pas encore l'objet d'une approche homogène dans le champ emploi formation. Dans le cadre de son offre de services de droit commun, le Cnam accompagne les auditeurs dans leur parcours de formation et leur propose une offre de service d'appui à la fois méthodologique et académique pour faciliter leur réussite. Ces services gratuits sont proposés au sein du centre de ressources et d'appui pédagogique, entité composée d'une équipe pluridisciplinaire d'enseignants. L'appui apporté consiste à donner aux auditeurs des points de repères pour gérer leur temps, organiser leur travail, faire un planning ou prendre des notes pendant les enseignements et lors de séances de soutien en petits groupes ou individuel permettant aux auditeurs de combler leurs lacunes dans certaines disciplines. Ce soutien est notamment proposé dans les unités d'enseignement (UE) de premier cycle, par exemple en mathématiques, physique, informatique, statistiques et en expression écrite ou outils de communication.

En conclusion, il existe une contribution potentielle, significative et cruciale des organismes de formation à la sécurisation des parcours professionnels. Elle est en train de se définir à la faveur d'essais et d'erreurs, d'identification des bonnes pratiques et d'intégration progressive de ces bonnes pratiques dans les actes métiers. C'est ce défi que le Cnam a commencé à relever.

Comment sécuriser les parcours professionnels ?

Stéphane Junique

Président, Harmonie mutuelle et VYV Care

À l'heure où les mutations du travail et les bouleversements sociétaux constituent des lames de fond sans précédent dans l'émergence de parcours professionnels et de vie plus fragmentés, la manière d'imaginer leur sécurisation est une véritable gageure collective. Parler des parcours professionnels, c'est parler des parcours de vie. À la pluralité des parcours, doivent répondre non pas une, mais des protections sociales où la personnalisation des réponses et de l'accompagnement ne rime pas avec une individualisation de leur financement. Les acteurs à but non lucratifs conjuguent de nombreux atouts pour répondre à ces enjeux de manière durable et responsable.

Les mutations de notre société ont conduit à un morcellement de la période d'activité, une pluralité des parcours et des phases de transition. Ces fluctuations créent des insécurités, notamment lors des périodes de transition. Au-delà d'un enjeu de politiques publiques, la sécurisation des parcours professionnels est un enjeu de société dont tous les acteurs doivent se saisir pour adapter les réponses aux besoins réels des individus pour les protéger et les rendre acteurs de leurs trajectoires.

Parler des parcours professionnels, c'est parler des parcours de vie. C'est cela qu'il faut aujourd'hui accompagner autrement, sur les plans individuel et collectif.

La transition du travail aux activités

Ces dernières années, le monde du travail, le marché de l'emploi et les formes d'activité ont connu de profondes mutations : fin du plein-emploi, mondialisation de l'économie et des échanges, croissance des inégalités (1), pluristatuts, digitalisation de l'économie, croissance de l'économie collaborative, développement du travail indépendant depuis 2009 avec la création du statut d'autoentrepreneur, importance stratégique grandissante de la « marque entreprise », etc.

Dans ce contexte, les travailleurs doivent adopter une démarche proactive constante quant aux éléments de sécurisation de leur parcours et prévenir les risques inhérents à des changements de situation plus fréquents. En parallèle, les préoccupations de la population ont également évolué, notamment vers la recherche d'un réel épanouissement personnel au travail, une moindre acceptabilité sociale des conséquences de la mondialisation, une conscience accrue des enjeux environnementaux, une attention portée à la responsabilité et à l'objet social des entreprises (la future loi Pacte, dite « loi entreprise » en est une manifestation clé) et vers une exigence accrue en matière de transparence et d'exemplarité. Les modalités des réponses aux conséquences de la fragmentation des parcours et notre rôle auprès des individus et des entreprises en sont ainsi modifiés.

Des mutations économiques subies

Le numérique, et notamment les nouvelles technologies, sont emblématiques de l'évolution du monde du travail et du marché de l'emploi que nous connaissons. À la fois créateurs et destructeurs d'emplois, ils remettent en cause les modalités de l'employabilité et l'obsolescence des compétences. La robotisation des lignes de caisses de supermarchés et autres points d'accueil est caractéristique de ce phénomène. Ces technologies ont également favorisé l'émergence de nouvelles formes d'emploi (micro-travail, travail parasubordonné, multiactivité, travail indépendant, etc…), sources d'insécurité nouvelle et d'instabilité potentielle. Ces évolutions, conjuguées à un engagement associatif qui n'a jamais été aussi élevé, font dire à certains que notre société n'est plus celle du travail mais celle des activités, qu'elles soient successives ou cumulatives, dans des secteurs différents, et parfois sous des statuts différents. Alors, comment sécuriser les parcours quand l'activité remplace l'emploi ? Comment sécuriser les parcours quand ne pas « être en emploi » accentue le risque face à la maladie et peut vouloir dire ne pas accéder au logement ? Comment accompagner le retour à l'emploi pour les personnes touchées par la maladie ? Comment accompagner les malades chroniques en entreprise ? Comment accompagner les entreprises dans leurs responsabilités vis-à-vis de leurs salariés ? Ces questions, non exhaustives, sont celles aujourd'hui posées par l'évolution des parcours.

Aux évolutions personnelles choisies

Au-delà de l'impact sur l'emploi et les formes de travail, les mutations sont aussi le reflet d'aspirations nouvelles, d'une quête d'épanouissement au travail à travers lequel l'individu veut trouver du sens. Cette quête explique aussi les changements de carrière, de secteur d'activité, de statut. Elle met potentiellement l'individu face à une rupture de ses droits, et crée des craintes en ce qui concerne ses charges familiales, immobilières, et la complexité réglementaire, etc. L'accord national interprofessionnel (ANI) était un élément de réponse pour les salariés du secteur privé. C'est aussi l'une des motivations du développement de la flexisécurité, entériné par la loi Travail d'août 2016.

Ces évolutions engendrent des trajectoires de plus en plus complexes et segmentées. Aux périodes d'activité succèdent des périodes transitoires plus ou moins longues et des réinsertions parfois difficiles, a fortiori pour des catégories plus fragiles (profils peu qualifiés, seniors, etc.). Face à ce constat, l'évolution de la protection sociale au sens large est un enjeu fondamental pour l'ensemble des acteurs de la société, au risque de devenir défaillante dans sa capacité à jouer un rôle d'amortisseur et d'investisseur social.

Mettre en place une ou des protections sociales ?

Si les parcours sont pluriels, doit-on parler d'une ou de protections sociales ? Pour être pertinente, cette question nécessite de prendre de la hauteur et de réfléchir aux besoins de la population, aux nouvelles problématiques auxquelles

notre société est confrontée, ainsi qu'aux réponses innovantes que l'on peut proposer.

Prendre en compte des besoins individuels

La vision classique de la protection sociale, liée à l'emploi et au statut qu'il confère à la personne, est dépassée. Notre approche doit être renouvelée pour mieux prendre en considération les individus dans leur globalité tout au long de leur vie. Il est donc nécessaire de remettre l'individu au centre pour sécuriser chaque trajectoire, « du berceau au tombeau », notamment dans les périodes transitoires. Si certains mécanismes répondent déjà à cette logique (portabilité et transférabilité), la démarche doit être approfondie.

Les besoins diffèrent et ne surviennent pas aux mêmes moments de la vie selon chacun. C'est pourquoi, pour être pertinent, l'accompagnement proposé doit être personnalisé et surtout être mené sur le long terme. En 2014, un rapport de l'Inserm démontrait qu'une personne modeste, seule ou avec un état de santé dégradé, a plus de difficultés à se projeter dans l'avenir, et par conséquent, à investir dans sa santé (2). L'environnement de travail est un déterminant clé des parcours de vie (maladies professionnelles, accidents du travail, rhumatismes, problèmes de dos, sédentarité, risques psychosociaux, mais aussi lien social, réalisation personnelle, etc.), face auxquels nous ne sommes pas égaux. La réflexion doit ainsi être menée en amont et en aval de la vie active, portée notamment par deux idées : la refondation de la protection sociale doit permettre de passer d'une égalité des chances à une égalité des possibles, tant dans l'accès à l'insertion que dans l'accès à une sécurité qui facilite des parcours choisis, et ce, sans obérer la qualité de vie postactivité, période d'autant plus clé aujourd'hui avec l'allongement de l'espérance de vie.

Cette vision reflète le souhait de chacun d'être considéré dans son individualité et de voir ses caractéristiques et ses multiples appartenances prises en considération (sexe, âge, territoire, entreprise, profession, situation familiale, etc.).

Une telle démarche aurait également pour avantage d'accroître le dynamisme des trajectoires. Des parcours mieux sécurisés poursuivraient un double objectif :

- maintenir et mettre en œuvre des droits et services répondant aux besoins des individus à travers une approche personnalisée de leur protection tout au long de leur vie ;

- permettre à chacun d'être plus maître de ses trajectoires.

Elle doit être source d'émancipation pour chacun.

Compte personnel d'activité et socle de solidarité

Dans une perspective d'évolution du modèle social, le compte personnel d'activité pourrait inspirer la création d'une protection sociale attachée à l'individu, plutôt qu'à son statut. Acquérir des droits tout au long de sa vie, et pouvoir les mobiliser lorsque le besoin s'en fait sentir, apparaît en adéquation avec les évolutions que nous connaissons et les besoins de la population. L'individu, au cœur du système, est le plus à même de construire ses propres trajectoires, si les moyens lui en sont donnés et si un accompagnement pertinent lui est proposé. En outre, le versement de points supplémentaires à certains profils précaires (jeunes sans qualification professionnelle, chômeurs de longue durée, etc.) poursuit également un objectif de réduction des inégalités, fondamental à l'heure où elles se creusent. C'est à cette condition que l'égalité des chances laissera réellement place à l'égalité des possibles et que les droits créés ne resteront pas théoriques.

Pour autant, permettre à l'individu d'activer sa protection quand il le souhaite n'a de sens que si elle s'appuie sur un socle universel et solidaire de droits sanctuarisés, garantissant une protection sur le long terme.

La solidarité doit permettre que personnalisation ne rime pas avec individualisation. Cela est d'autant plus justifié que les déterminants du bien-être sont multifactoriels, individuels autant que collectifs. Sur le plan collectif, la considération croissante pour la santé environnementale en est une manifestation. Sur le plan individuel, un tel système doit favoriser l'adoption de comportements responsables. Cela nécessite de faire évoluer le système de santé, du soin à une approche par les déterminants de santé. Investir la dimension préventive c'est rappeler que la santé est un risque long. C'est un capital qui se construit, se cultive et se protège. La mise en place d'actions de prévention, de sensibilisation et d'éducation à destination du public, de nos adhérents, notamment dans le cadre professionnel, prend là tout son sens.

En outre, l'enjeu d'une nouvelle approche de la protection sociale est de lutter plus fortement contre les inégalités et la précarisation de certaines catégories. Dans ce contexte, la solidarité et la mutualisation, couplées à la personnalisation de l'accompagnement dans l'activation des leviers de protection et de sécurisation, doivent rester l'assise première du modèle, afin de garantir un accès à la protection sociale qui ne soit pas tributaire de la seule capacité contributive des individus.

Un tel dispositif serait plus transparent, lisible et efficace. Trop de personnes renoncent encore à des droits ou des aides en raison de la complexité des démarches à effectuer, voire tout simplement par manque d'information. Le faible taux de recours à l'aide au paiement d'une complémentaire santé (ACS) et à la couverture maladie universelle (CMU) en est un bon exemple. Il n'est d'ailleurs pas anodin que certains programmes et débats de l'élection présidentielle aient porté sur le revenu universel.

Enfin, la lutte contre les inégalités est l'affaire de tous. D'autant qu'une citoyenneté plus active est à l'œuvre (par exemple, pétitions citoyennes au niveau du Conseil économique social et environnemental), que de nouvelles solidarités s'organisent, et que les réponses, plurielles, doivent être élaborées à travers des stratégies d'alliance autour d'acteurs animés dans l'action par la recherche première d'une utilité sociale avérée. C'est l'attachement à ces valeurs qui guide l'action d'Harmonie mutuelle, et plus largement celle de l'économie sociale et solidaire. L'État n'est pas le seul acteur de la solidarité.

La pertinence d'une réponse non lucrative

À l'heure où une certaine défiance existe envers les acteurs institutionnels traditionnels et où les attentes de la société en matière de transparence et d'exemplarité se renforcent, la création d'un pôle de solidarité active en matière de santé et de protection sociale constitue une véritable plus-value, garante d'une action engagée sur le long terme.

Une alliance pour l'action

Le modèle de gouvernance et d'entreprendre non lucratif (ou à lucrativité limitée) propre à l'économie sociale et solidaire est la condition sine qua non à une utilité sociale durable responsable au bénéfice du plus grand nombre. Atypiques nous sommes, atypiques nous resterons. Sans actionnaires, nous n'avons ni vocation à faire des bénéfices, ni vocation à être déficitaires. C'est une « économie des communs » et du bien-être que nous construisons au sein d'Harmonie mutuelle et avec le groupe VYV. Réinvestir nos excédents dans des innovations sociales au service des adhérents, être solide et durable dans l'accompagnement, construire une véritable fabrique non lucrative de protection sociale collective : notre ambition est de participer à la création d'un nouveau système de protection, élaboré pour et par les usagers.

Créé en septembre 2017, le groupe VYV constitue le noyau de ce qui pourrait constituer un pôle de solidarité active. Espace de synergie entre plusieurs acteurs et réseaux (Harmonie mutuelle, Istya, MGEN, structures de soins et services d'accompagnement), il

regroupe une multitude d'offres, plus d'une vingtaine de métiers (offres, services et accompagnement en matière de santé, de prévoyance et de prévention, mais aussi épargne retraite, assurance emprunteur, Livre III [3], etc.), capables d'intervenir sur différents pans du parcours de santé et de vie et d'accompagner plus de dix millions d'adhérents. L'action d'un tel pôle a comme horizon celui d'une réponse responsable aux besoins. Parmi nos dernières réalisations, l'assurance emprunteur comme notre investissement dans *mesdocteurs.com* témoignent de cette approche globale.

Une empreinte mutualiste éprouvée

Même s'il nous faut aller plus loin, cela n'est pas nouveau pour nous. Harmonie mutuelle s'engage dans l'accompagnement de ses adhérents et de ses entreprises clientes. Envisagée de manière globale, la sécurisation des parcours professionnels doit nous questionner sur l'entreprise, son rôle, sa responsabilité et ses besoins. D'autant qu'avec l'ANI, la place de l'entreprise s'accroît sur ces sujets. Notre rôle sera de plus en plus de les accompagner dans leurs responsabilités vis-à-vis de leurs salariés (qualité de vie au travail, actions de prévention, relocalisation d'emplois, réflexions partagées sur les enjeux de la protection sociale en entreprise, responsabilité sociétale et environnementale, évolutions réglementaires comme le compte pénibilité). La performance économique ne doit en effet pas se faire au détriment de la performance sociale. Le développement du bien-être en entreprise a également pour finalité d'engager le salarié dans l'entreprise et de lui permettre d'y trouver un épanouissement personnel bénéficiant aussi, in fine, à l'entreprise (taux d'adhésion à la stratégie plus fort, baisse de l'absentéisme). Santé au travail et santé du travail vont de pair !

Enfin, la lutte contre les inégalités territoriales dans laquelle nous sommes également engagés, est centrale. Plus de 4 500 collaborateurs et 1 700 élus chez Harmonie mutuelle contribuent au dynamisme territorial sur tout le territoire français. Dès 2019, ils seront 2 000. Une stratégie ambitieuse mais qui participe à un accompagnement de proximité, à une citoyenneté active et à la sécurisation des parcours.

Notes

1. En 2017, selon une étude d'Oxfam, 1 % de la population mondiale se partageait 82 % de la richesse totale.

2. Inserm, Inégalités sociales de santé en lien avec l'alimentation et l'activité physique*, 2014.*

3. Le livre III concerne les mutuelles et unions pratiquant la prévention, l'action sociale et la gestion de réalisations sanitaires et sociales. Ainsi, à travers VYV Care, ce sont plus de 900 structures de soins et services d'accompagnement et 17 métiers à disposition de nos adhérents et des citoyens (Ehpad, crèches, centres hospitaliers, centres optiques, dentaires...).

4.

Études et débats

***Les débats de* Risques**

Actualité de la Fondation du risque

Livres

Les coûts du risque une vieille histoire ?

Pierre Martin

Agrégé d'histoire, docteur en histoire

« L'incertitude est une méconnaissance » estimait le mathématicien Bernoulli au début du XVIIIe siècle : une méconnaissance qui interdirait un calcul cohérent du prix du risque. Le risque a certes un prix calculé a priori par l'assureur, mais il a aussi des coûts, révélés souvent a posteriori. Sans oublier que la distinction canonique entre le risque et l'incertitude est postérieure d'un siècle à la création des sociétés d'assurance en France ! Comme souvent, le détour par le passé permet, sans doute, d'éclairer le présent...

Le risque : un prix probabilisable

L'évaluation du prix du risque obéit apparemment à un calcul rationnel aujourd'hui bien maîtrisé, du moins en assurances dommages type incendie, accidents et risques divers. Nous laisserons ici de côté l'assurance santé, qui est un risque de type Veblen (1) dont le prix croît davantage que le revenu en ce qu'il s'agit d'un marché du bien-être (2). Un assureur se réfère aujourd'hui à un protocole qui a le mérite de la simplicité. Le *Manuel International de l'assurance*, une bible de l'assurance, distingue ainsi trois périmètres concentriques à la cotisation ou prime d'assurance qui évalue le prix du risque. La cotisation pure, dite encore cotisation d'équilibre ou cotisation technique, correspond à la « part des sinistres dans la mutualité gérée par l'assureur. (3) » La cotisation nette ou cotisation commerciale désigne la cotisation pure à quoi s'ajoutent les frais de l'assureur et sa marge bénéficiaire. La cotisation totale correspond à la cotisation nette augmentée des taxes et impôts collectés par l'assureur, comme des surprimes éventuelles destinées à alimenter un fonds. Ainsi de la surprime assise sur les contrats multirisques habitation destinée à alimenter le fonds de garantie pour les attentats. Le calcul du coût de la cotisation pure obéit grossièrement à un calcul de probabilités d'autant plus robuste qu'il est assis sur une base large, la mutualité des risques constituée par la somme des risques endossés par l'assureur. Pour cela, l'assureur raisonne en termes de risque, non d'incertain. Cette distinction essentielle n'a été clairement énoncée qu'en 1921 par John Maynard Keynes (4) et Franck Knight (5). Le risque est probabilisable quand l'incertain ne l'est pas. Le risque peut donc avoir un prix à l'inverse de l'incertain. Denis Kessler, actuel président-directeur général de Scor, donnait un exemple fameux pour comprendre ce qui sépare ces deux univers. Savoir si je suis exposé au risque du VIH relève de mes

pratiques sexuelles, plus ou moins risquées, probabilisables donc. Savoir quand on découvrira un remède durable contre le virus du VIH relève de l'incertain, tant les paramètres sont flous, à commencer par la nature du virus du VIH qui détruit le système immunitaire et empêche de raisonner en termes de vaccins. Une fois le périmètre du risque posé, on entre dans la sphère de l'assurable. Reste à élaborer une tarification. L'assureur évalue alors la mutualité agglomérée des risques sur laquelle il pense travailler et fait appel à des actuaires chargés d'évaluer le sinistre maximum possible (SMP), la pire probabilité de réalisation du risque. Le sinistre maximum possible désigne donc « en assurance et risques divers, […] le montant maximum mis à la charge de l'assureur en cas de sinistre se produisant dans les circonstances les plus défavorables et pouvant atteindre une communauté de risques ou des risques proches de moins de dix mètres (6) ». Ainsi les assureurs dommages avaient-ils envisagé le crash d'un avion de ligne sur le centre-ville d'une mégapole massivement assurée comme New York... Un avion, pas deux avions en même temps et au même endroit ! Le système financier de la réassurance mondiale a alors manqué de sauter sur ce méga-sinistre qui relevait de la marge d'erreur. Cela posé, l'assureur évalue un coût statistique moyen qu'il peut affiner en fonction de sa moindre asymétrie d'information quant au risque endossé. Typiquement, un automobiliste qui peut arguer d'un passé de bon conducteur auprès d'une société d'assurance verra son tarif minoré par un bonus, et inversement un mauvais conducteur verra sa prime majorée d'un malus pour prendre en compte le moindre coût ou le surcoût potentiel du risque.

Quel que soit le type de risques, le calcul du prix s'insère dans une sorte de triptyque. Le premier volet concerne la prévention et la précaution. Pour échapper à l'incertitude, il faut susciter une certaine prudence. C'est tout l'objet des franchises qui déterminent un reste à charge incompressible payé par l'assuré. Les premiers statuts des compagnies d'assurance incendie de la Restauration imposaient tous pareilles clauses, (7) accompagnées de formules consacrées quasi identiques quelles que soient les sociétés : « car l'assuré ne saurait en aucun cas s'enrichir à l'assurance. » Bref, une partie du coût du sinistre – en général 5 % –, est assumée par le souscripteur. Pour maîtriser le coût du risque, il faut museler l'aléa moral sans quoi l'assurance paie sans limites, ce qui fait exploser le coût du risque. L'hypothèse selon laquelle « l'assurance paiera », définition commune de l'aléa moral, revient à déplafonner à l'infini le coût du risque. Le deuxième volet repose sur la mutualisation des risques, c'est-à-dire sur leur partage potentiel. L'économiste Pierre-André Chiappori en propose une définition élégante : « La mutualisation consiste à regrouper un grand nombre de risques indépendants à l'intérieur d'une structure commune. […] Le principe fait appel à la loi des grands nombres et à l'idée que, sur une population de référence suffisamment importante, le nombre agrégé d'accidents est plus ou moins constant (8). » Si la mutualisation est correctement constituée, le risque correspondant est alors « globalement éliminable » pour reprendre le mot du Nobel d'économie Maurice Allais. L'assureur neutralise donc le risque moyennant une prime. Il endosse des risques d'autant plus facilement que le prix du risque est correctement évalué : il permet à des porteurs de risques riscophobes de se défausser du risque moyennant un prix, qui est aussi celui de la tranquillité... Le troisième volet consiste à partager des risques globalement inéliminables et non plus à agréger des risques éliminables. Il s'agit de risques d'importance majeure tel un tremblement de terre dans un espace densément assuré comme la Côte d'Azur ou la Californie, toutes deux surexposées aux risques sismiques. Reprenons le cas d'une assurance habitation. Le coût du risque intègrera ici celui de la réassurance, dont l'assuré ne sait rien. La réassurance permet de transférer, de partager le risque avec un réassureur qui interviendra au-delà d'un seuil mesuré en coût global du sinistre ou au-delà d'un pourcentage des sinistres mesurés par rapport aux primes encaissées dans l'année. Les sociétés de réassurance existent ainsi depuis la fin du XIXe siècle (Swiss Re est fondée en 1863, Munich Re en 1880), mais l'économiste libéral français Frédéric Bastiat avait suggéré pareils transferts de risques mondialisés dès 1850 dans *Harmonies économiques* : « Les compagnies

s'assurent entre elles par les réassurances, de sorte qu'au point de vue de la réparation des sinistres, qui est le fond du phénomène, mille associations diverses établies en Angleterre, en France, en Allemagne, en Amérique, se fondent en une grande et unique association (9) ». Bastiat, avec trois quarts de siècle d'avance sur la théorie économique, avance que l'« aversion pour l'incertitude » de la personne explique l'association des personnes (10). En définitive, l'économie de l'assurance nous enseigne que le coût du risque relève d'une approche rationnelle, probabilisable, rassurante somme toute. Et ce d'autant plus que les méthodes de calcul se sont améliorées, que l'expérience accumulée permet de déterminer un coût de plus en plus rigoureux du risque.

Le risque : un prix contestable (II)

En réalité, il faut déjà rappeler que les assureurs ont pendant un siècle élaboré des tarifications sans avoir à leur disposition les concepts de risque et d'incertain. Ils en avaient compris l'essentiel et procédaient par tâtonnements, et endossaient réellement des risques auxquels ils donnaient un prix cohérent : ces sociétés ont survécu et sont même devenues des actrices majeures au XXIe siècle. Citons pour la France AXA – dont l'ancêtre est l'Ancienne mutuelle (1817) –, le groupe des Mutuelles du Mans qui rassemble feu le Groupe Azur issu de l'Assurance Mutuelle de la Seine et de la Seine-et-Oise (1819) (12) et les Mutuelles du Mans nées dans la Sarthe en 1828... Les assureurs du XIXe siècle étaient donc des praticiens, non des théoriciens du risque, qui sont malgré tout arrivés à construire un prix cohérent du risque. Rappelons que le cadre juridique leur était très favorable. Il n'y avait en effet pas de loi spécifique sur le contrat d'assurance avant celle du 13 juillet 1930 (13). L'assuré était largement captif et le contrat, de cinq années en assurance incendie (l'ancêtre des contrats multirisques habitation), ne pouvait être dénoncé par le souscripteur, sauf à devoir renoncer aux garanties... tout en demeurant assujetti au paiement de la prime ! La vente d'un bien immobilier et le transfert de propriété ne permettaient même pas de se défaire du contrat qui restait attaché au bien pour toute la durée de souscription. Inversement, les clients qui dissimulaient des risques, omettaient de prévenir leur assureur de changements de périmètre ou de destination, se voyaient résiliés. On peut schématiquement distinguer deux types de tarification pratiquée. Les sociétés d'assurance par actions, cotées, calculaient une prime généreuse, correspondant à un tarif moyen, en échange de quoi elles couvraient assez volontiers. Les sociétés d'assurance mutuelle avaient une connaissance beaucoup plus fine du risque, assises initialement sur des marchés souvent départementaux très bien connus, et sur de bons risques sélectionnés à la souscription. Du coup, elles étaient beaucoup moins chères, d'autant qu'elles n'avaient pas d'actionnaires à rémunérer. Un économiste contemporain dirait qu'elles pratiquaient un prix prédateur, cohérent cependant par rapport à leur modèle économique. Les archives historiques des AGF, aujourd'hui fondues dans Allianz France, conservent de précieux carnets d'agences où les agents, par circonscription commerciale, tenaient entre autres une rubrique « concurrence ». Les mentions concernant les mutuelles, notamment les « grosses mutuelles » du Mans dans le grand Ouest et l'Assurance Mutuelle de la Seine et de la Seine et Oise (AMSSO) sont concordantes. Ainsi l'agent d'Étampes note en 1862 : « La Mutuelle AM occupe à Étampes le premier rang grâce aux primes réduites de ses tarifs ». Une manière pour les agents de se dédouaner par rapport à leur hiérarchie ? La remarque est pourtant réitérée en 1863, 1868, 1874, 1899... Un agent de Seine-et-Oise se désole ainsi en 1860 : « Notre concurrence la plus intraitable est la mutuelle AMSSO. Nous luttons avec elle dans les campagnes, mais dans les villes elle a tout absorbé depuis longtemps. (14) » Ce prix moindre pour des garanties équivalentes explique la constitution de marchés sanctuarisés dans le Grand Bassin parisien pour l'AMSSO et dans l'Ouest pour les Mutuelles du Mans. Du « *low cost* (15) » avant l'heure. Plus exactement le premier âge du « *low cost* » pour des mutuelles « de droite » composées de propriétaires qui mettaient

en commun leurs fortunes contre l'infortune sur le marché de l'assurance incendie. Le deuxième âge est celui de la Maaif (Mutuelle d'assurance automobile des instituteurs de France) et de la GMF (Garantie mutuelle des fonctionnaires) nées un siècle plus tard en 1934 sur le marché alors balbutiant de l'automobile. Il s'agit à l'origine de mutuelles « de gauche », parfois anticapitalistes (16), qui entendaient contester les rentes de monopole des assureurs en place par des prix bon marché. Finalement, le prix du risque obéirait à une dynamique paradoxale de l'assuré. D'un côté, le client souhaite une prise en charge de risques de plus en plus étendue, preuve qu'il est prêt à payer une prime pour se défausser sur un assureur. D'un autre côté, il recherche le moindre prix pour des garanties équivalentes. Une première faille dans l'approche rationnelle du prix du risque ?

Le risque : un coût impensable

En réalité, l'irrationnel côtoie le rationnel dans cette affaire. Rappelons d'abord que le prix du risque n'est qu'une contrepartie monétaire qui donne, faute de mieux, un prix aux choses. Ce prix de marché est à la base du mécanisme assuranciel de dédommagement. Pour l'assuré, un meuble de famille, un bijou transmis de génération en génération, un bien immobilier restauré avec patience ne correspondent jamais au remboursement de l'assureur. Et que dire de la perte d'un bras ou d'une jambe ? Les débuts de l'assurance accidents du travail en France à compter de la loi d'avril 1898, magnifiquement restaurée par le travail considérable de François Ewald, (17) révèlent les limites de la monétarisation du risque. Certes, la loi instaure le premier État providence en France qui couvre les risques d'accidents du travail en donnant un prix au risque. De plus cette loi est élargie aux maladies professionnelles dès 1919. Enfin le risque accidents du travail et maladies professionnelles (ATMP) devient la quatrième branche de la Sécurité sociale, avec retard, à compter du 1er janvier 1947. L'ouvrier, les salariés en général gagnent au change. Jusque-là considérés responsables d'eux-mêmes sur leur lieu de travail, ils sont désormais couverts par leur employeur, que celui-ci se défausse sur une compagnie moyennant le paiement de la prime ou que le patron choisisse de s'autoassurer. Mais quel prix donner à une jambe ou un bras arraché par une machine à l'usine ? L'assureur, faute de mieux, calcule le taux d'invalidité et compense le handicap par le versement d'une rente correspondant au pourcentage d'incapacité durable de travailler. Vieille histoire en réalité dont les fondements avaient été posés avec clarté par Jean-Baptiste Colbert au début du règne de Louis XIV. Le jeune Bourbon avait promu Colbert ministre des Finances au début de son très long règne (1661-1715). Ministre de 1661 à 1683, Colbert définit le prix du risque de façon très paradoxale. D'un côté, il interdit durablement l'assurance sur la vie, attendu que « l'homme étant hors de prix, sa vie ne saurait être objet de commerce ». Le juriste Portalis, alors qu'il travaille sur le Code civil publié en 1804, considère encore que « ces espèces de pactes sur la vie ou la mort d'un homme sont odieux, et ils ne peuvent être sans danger. La cupidité qui spécule sur les jours d'un citoyen est souvent bien voisine du crime qui peut les abréger (18). » D'un autre côté, Colbert par une ordonnance de 1686, autorise la création d'une assurance maritime qui devait (sans grand succès) ramener les marchands français s'assurer en France et non à l'étranger. Colbert raisonne ici en mercantiliste et non en libéral : le prix est un paramètre accessoire de ses catégories de pensée. Enfin Colbert instaure en 1673 le Fonds des invalides de la marine. L'idée est que les marins devenus incapables de vivre de leur travail, du fait de leur invalidité, sont pensionnés par l'État. Le sang a un prix, d'autant plus inestimable s'il est mis au service de la nation. Ce qui justifie l'exemption fiscale de la noblesse vaut aussi pour les soldats blessés. « Ancêtre de l'actuel Établissement national des invalides de la marine (Enim), ce fonds a été créé en compensation de l'enrôlement. Il avait vocation à financer des hospices maritimes, au travers d'un faible prélèvement sur la solde des marins. En 1689, ce secours aux marins estropiés a évolué vers le versement d'une demi-solde, qui constitue

l'ancêtre de la pension d'invalidité (19) ». Colbert élargit en réalité aux marins le concept de l'Hôtel des Invalides défini par l'ordonnance royale du 24 mai 1670 destiné aux militaires inaptes à la guerre. Dédommagement, pension, demi-solde, capital : le prix du risque paraît bien dérisoire au regard d'une amputation du corps, voire de la perte d'un être cher. Telle est pourtant la limite ultime de l'assurance qui rend dérisoire la notion de prix au sens monétaire.

Le risque a donc un prix, que les assureurs apprennent à calculer rationnellement, et de plus en plus rigoureusement. Actuaires et statisticiens affinent donc sans cesse le prix du risque. Pourtant, ce prix n'a cessé d'être contesté par de nouveaux offreurs, singulièrement les mutuelles au XIXe siècle et au XXe siècle. Demain l'oligopole des Gafa (Google, Amazon, Facebook, Apple) poussera sans doute les spécialistes du *big data* à calculer un prix du risque « sur mesure ». Ce qui posera des problèmes considérables d'éthique et de fonctionnement, puisque ce « recalcul » ad hoc contredit le principe même de la mutualisation. En définitive, le prix du risque bute in fine sur la définition monétaire du dédommagement qui n'est qu'une piètre compensation au regard du handicap ou, pire, du décès. Sans parler de risques considérables auxquels on ne pourra guère trouver de prix, ou de couverture. Le risque amoureux est ainsi, peut-être, le risque maximal par essence. C'est ce que pensent les avocats en charge des divorces, mais déjà au XVIIe siècle La Rochefoucauld dans sa maxime 47 : « La prudence et l'amour ne sont pas faits l'un pour l'autre : à mesure que l'amour croît, la prudence diminue (20) ».

Notes

1. Thorstein Veblen, The Theory of the Leisure Class*, 1899. Traduction française* Théorie de la classe de loisir*, TEL Gallimard, 1970, préface de Raymond Aron.*

2. Arthur Cecil Pigou, The Economics of Welfare*, Macmillan, 1920.*

3. Jérôme Yeatman, Manuel International de l'assurance*, Economica, 1998, p. 33.*

4. John Maynard Keynes, A Treatise on Probability*, 1921.*

5. Franck Knight, Risk, Uncertainty and Profit*, 1921.*

6. Martine Charre-Serveau et James Landel, « Lexique des termes d'assurance », L'Argus*, 2000, p. 347.*

7. Pierre Martin, Deux siècles d'assurance mutuelle. Histoire du groupe Azur 1819-2000*, CTHS, Histoire, 2009.*

8. Pierre-André Chiappori, Risque et assurance*, Flammarion, 1997, p. 32.*

9. Fréderic Bastiat, Harmonies économiques*, chapitre 14, « des salaires », 1850.*

10. Georges Lane, « Bastiat, l'aversion pour l'incertitude et la loi de l'association », in Journal des économistes et des études humaines*, volume XI, numéro 2/3, juin-septembre 2001, pp. 415-450.*

11. William Baumol, John Panzar et Robert Willig, Contestable Markets and the Theory of Industry Structure*, 1982.*

12. Pierre Martin, Deux siècles d'assurance mutuelle. Histoire du groupe Azur 1819-2000*, CTHS, Histoire, 2009.*

13. César Ancey et Lucien Sicot, La loi sur le contrat d'assurance. Loi du 13 juillet 1930*, LGDJ, 1955.*

14. Pierre Martin, Deux siècles d'assurance mutuelle. Histoire du groupe Azur 1819-2000*, CTHS, Histoire, 2009, p. 137.*

15. Emmanuel Combe, Le low cost*, La Découverte, coll. « Repères », 2011.*

16. Michel Chaumet, Maif, l'histoire d'un défi*, Le Cherche Midi, 1998.*

17. François Ewald, Histoire de l'État providence : les origines de la solidarité*, Grasset, 1996.*

18. Portalis, Travaux préparatoires au Code Civil de

1804, cité in *Michèle Ruffat, « L'assurance française et sa tutelle. Structures administratives et modes de régulation de l'Ancien Régime à la Seconde Guerre mondiale »,* in *Borscheid, Plessis, Frax (dir),* Insurance in Industrial Societies : Econmic Role, Agents and Markets from 18th Century to Today, *Clara Eugenia Nunez Editor, 1998, p. 59.*

19. Francis Delattre, Sénat, commission des Finances, « Rapport d'information sur le régime spécial de retraite et de Sécurité sociale des marins (Enim) », 2 juillet 2013.

20. La Rochefoucauld, Maximes, *1re édition 1664, texte établi par Jacques Truchet, réédition Garnier, 1967, p. 171.*

Les modèles prédictifs peuvent-ils être loyaux et justes ?

Arthur Charpentier

Professeur, Université de Rennes 1

Dans Nosedive *(traduit par le titre* Chute libre *en France), le premier épisode de la saison 3 de la série télévisée* Black Mirror*, on découvre la dystopie d'une société régie par une « cote personnelle », une note, un score allant de 0 à 5. Dans ce monde, chaque personne note les autres, les mieux notés ayant accès à de meilleurs services (priorité dans les services, meilleurs taux, meilleurs prix, etc.). Cette tendance à construire des scores dans toutes sortes de domaines (historiquement sur les crédits mais aujourd'hui sur des aspects criminels, voire civiques dans certains pays) ne va-t-elle pas déboucher sur un monde qui serait un concours de popularité sans fin ? Et comment serait-elle conciliable avec une justice sociale, a priori souhaitable ?*

Les scores de crédit et les réseaux sociaux

Un score de crédit est, d'un point de vue actuariel, une grandeur proportionnelle à la probabilité de ne pas honorer ses engagements en tant que créditeur. Cela peut être de ne plus pouvoir payer les échéances pendant trois mois consécutifs, ou juste d'avoir un retard. Dans la vraie vie, comme toujours, c'est un peu plus compliqué. Aux États-Unis ou en Grande-Bretagne, il n'est pas rare que les étudiants s'endettent sur des dizaines d'années pour avoir l'opportunité de suivre les cours qui les intéressent (même si la motivation est surtout d'obtenir un diplôme en fin de parcours). Mais surtout, dès qu'ils atteignent l'âge de dix-huit ans, des sociétés de notation de crédit vont surveiller tous leurs déplacements. Souvent à leur insu. Et si un jour, un crédit consommation ou hypothécaire est refusé, les raisons ne sont jamais motivées. Est-ce dû à un retard dans un paiement de loyer ? à des amendes de bibliothèque oubliées ? à une facture d'eau impayée, vieille de plusieurs années ?

Les sociétés de notation de crédit aux États-Unis, mais aussi en Chine, commencent à étudier la possibilité d'utiliser des données provenant de médias sociaux pour améliorer le score de crédit. Compter le nombre de fois où un utilisateur utilise le mot « gaspillé » (« *wasted* » en anglais) dans ce qu'il poste en ligne ne peut-il pas révéler une information quant au remboursement de dettes ? C'est en tout cas ce que prétend l'analyste de crédit américain Fico : « *If you look at how many times a person says "wasted" in their profile, it has some value in predicting whether they're going to repay their debt (...) It's not much, but it's more than zero* » [McLannahan, 2015]. En Chine, le prêteur *peer-to-peer* Jubao a révélé qu'il était plus susceptible de donner des « bonus » aux emprunteurs s'ils étaient des amis Facebook avec des célébrités, tel que le raconte Botsman [2017].

Pour l'instant, les sociétés de notation de crédit utilisent encore les données qu'elles connaissent bien (factures de services publics et cartes de crédit), mais elles imaginent que bien des informations intéressantes doivent être accessibles (d'une manière ou d'une autre) sur les réseaux sociaux. Mais les données sont encore rares, et difficiles à analyser. Quid de la composante sarcastique ou humoristique (1) dans un tweet utilisant le mot « *wasted* » ? Comme souvent, la difficulté est que les données réellement pertinentes sont difficiles à obtenir. S'il est possible d'avoir des informations sur le paiement du loyer quand un locataire passe par une agence, que faire pour les transactions entre deux particuliers ? Et si c'était possible, comment traiter le cas de colocataires ? Ne pas obtenir de crédit parce qu'un ancien colocataire n'a pas payé dans les temps devient dérangeant. D'autant plus s'il s'agit peut-être d'une facture de téléphone cellulaire réclamée abusivement par la compagnie de téléphonie, alors que l'abonnement avait été résilié.

Mais le gros « malus » dans le score de crédit est bien souvent le fait de ne jamais avoir eu de carte de crédit. On pourrait penser qu'une personne qui n'a pas eu besoin d'une carte de crédit (et se contentait d'une carte de débit, permettant d'acheter chez un commerçant, comme la majorité des cartes bancaires en France) est le propre d'une personne prudente, qui n'a pas besoin de crédit pour des dépenses quotidiennes. Mais pour les établissements de crédit, cette personne n'est pas fiable car on ne la connaît pas. Et c'est à elle de prouver qu'elle l'est (on revient à la pratique récurrente d'inversion de la charge de la preuve évoquée dans Charpentier [2016]). C'est étrangement ce qui se passe aujourd'hui quand on veut entrer sur le sol américain sans avoir de page Facebook.

Dans un monde de surveillance généralisée

Et si les établissements de crédit n'étaient pas les seuls intéressés par notre vie ? Que serait un monde si, en plus de savoir si je paie mes factures à temps, certains cherchaient à connaître mes réseaux d'amis, à savoir quels journaux je lis, si je préfère acheter du lait entier ou du lait demi-écrémé ? Quand on visite le musée de la Stasi à Berlin, on découvre que ce monde a existé, qu'une personne sur soixante-trois était agent (ou indicateur) de la Stasi (en comptant les indicateurs occasionnels, la proportion peut atteindre une personne sur six). Le musée décrit un panoptisme total, chacun étant observé en permanence, comme le décrit Foucault [1975].

Mais ce cauchemar ne correspond-il pas à notre monde actuel, de surveillance permanente, plus ou moins consentie. Surveillance via les téléphones cellulaires (géolocalisation pour la fonction la plus courante, mais parfois aussi des enregistrements audio à l'insu de l'utilisateur par certaines applications), via les objets connectés, mais aussi les caméras de surveillance couplées à des algorithmes de reconnaissance faciale de plus en plus performants. Fin 2017, en Chine, 170 millions de caméra étaient installées, et le cap des 300 millions devrait être atteint d'ici 2020. Lors d'une expérience tentée par la BBC (2), il a fallu sept minutes pour retrouver le journaliste John Sudworth qui se promenait dans les rues.

Le danger est que l'on ne sait jamais trop qui contrôle. De plus en plus de compagnies privées de sécurité se sont associées aux gouvernements. Les fournisseurs de messageries électroniques lisent nos messages pour détecter du spam, mais aussi pour revendre certaines informations. Par exemple, dans les règles de confidentialité annexées aux conditions générales d'utilisation de Gmail (Google) on lit : « Nos systèmes automatisés analysent vos contenus (y compris les e-mails) afin de vous proposer des fonctionnalités personnalisées sur les produits, telles que (...) des publicités sur mesure ». Les assureurs envisagent de plus de plus l'installation de boîtiers GPS dans les voitures, mais en passant par des prestataires externes. Au-delà de la propriété des données (évoquée dans Charpentier et Suire [2016]), on peut s'interroger sur leur revente et leur utilisation. Savoir que quelqu'un se rend régulièrement dans un centre de transfusion sanguine est une information potentiellement intéressante, surtout couplée à d'autres.

Depuis 2014, le gouvernement chinois travaille sur un système d'évaluation de ses propres citoyens programmé pour être mis en place en 2020, comme le raconte Trujillo [2017]. Ce « système de crédit social » vise à créer un « score citoyen » (pour reprendre l'expression de Galeon et Bergan [2017]), afin de prédire, et prévenir, les dangers potentiels, normalisant les conduites individuelles par des dispositifs panoptiques (par exemple la vidéosurveillance), induisant des réflexes d'autodéfense et d'autocontrôle. Comme le disait Foucault [1975], il s'agit de « faire que la surveillance soit permanente dans ses effets, même si elle est discontinue dans son action ; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice » (même si souvent, aujourd'hui, elle est en plus continue dans son action). Certains de ces scores sont utilisés par la police pour savoir où patrouiller pour faire baisser la criminalité, comme PredPol. Mais quand on y regarde de plus près, les prédictions disent, en substance, que les crimes auront lieu (en majorité) dans les zones (historiquement) les plus criminogènes de la ville. La frontière entre la banalité et la tautologie est étroite. Et le réel danger est que, bien souvent, les scores transforment les probabilités en quasi-certitudes, et le soupçon devient une preuve, comme le notait Supiot [2015].

Justice prédictive et méthodes actuarielles

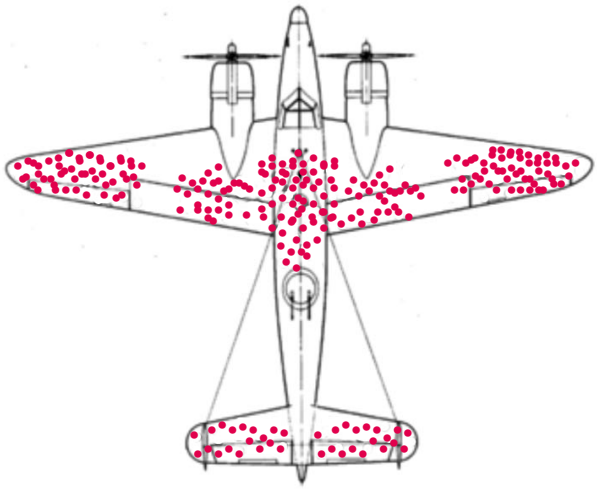
En juin 2010, un rapport de l'Académie de médecine préconisait d'« améliorer la pratique des expertises de dangerosité des criminels sexuels en enseignant et en diffusant les méthodes actuarielles » [Binet, 2010]. Ces méthodes actuarielles sont tout simplement les techniques de *scoring*, de profilage tel que le définit le Règlement européen relatif aux données personnelles du 27 avril 2016 (RGDP). Angèle Christin s'est intéressée aux algorithmes qui estiment la probabilité de récidive dans la justice pénale américaine. Comme elle l'a montré, ces techniques posent nombre de questions, en particulier des biais discriminatoires, l'opacité qui rend difficile les recours, et surtout la difficulté de comprendre ce qui est réellement calculé. Dans l'État de Virginie, un score entre 1 et 10 est renvoyé, convention reprise par Compas (Correctional Offender Management Profiling Alternative Sanctions) qui offre en plus un code couleur qui prédit le risque de récidive violent. Il s'agit alors d'un outil d'aide à la décision, une machine ne pouvant placer une personne en détention seule [Christin *et al.*, 2015].

Les conclusions d'un score prédictif dépendent de deux éléments clés : le modèle utilisé, et les données. Dans la majorité des cas aux États-Unis, les codes des modèles restent opaques (et donc impossibles à attaquer), et rares sont ceux qui ont vu les données utilisées pour calibrer ces modèles. Mais on peut se demander si les décisions de justice ne sont pas elles aussi relativement opaques ? Certes, les juges doivent motiver leurs décisions, ce qui les rend critiquables et attaquables, mais si le processus était si transparent, les issues d'un procès ne devraient-elles pas être alors davantage prévisibles ? Enfin, les différents biais sont assez simples à comprendre. Supposons qu'être riche permet d'avoir un bon avocat, et avoir un bon avocat permet de ne pas avoir certaines condamnations. Dans ce cas, une variable liée à la richesse (le type de véhicule possédé par exemple) sera liée positivement avec le fait de ne pas être coupable (reconnu coupable), et fera baisser le « score de dangerosité ». L'autre danger dans les biais de sélection est qu'ils sont parfois complexes à comprendre, voire paradoxaux. Un exemple classique est celui illustré dans la figure 1 (voir p. 110). Pendant la Seconde Guerre mondiale, il a été demandé à des ingénieurs et des statisticiens comment renforcer les bombardiers qui faisaient face au feu ennemi.

Le statisticien Abraham Wald a commencé à collecter des données sur les impacts sur la carlingue, comme le raconte Mangel et Samaniego [1984]. À la surprise générale, il a recommandé de blinder les endroits des appareils qui présentaient le moins de dommages. En effet, les avions utilisés dans l'échantillon présentaient un biais important : seuls les avions

revenus avaient été pris en compte. S'ils avaient pu revenir avec des trous au bout des ailes, c'est que ces parties étaient suffisamment solides. Et comme aucun avion n'était revenu avec des trous au niveau des moteurs des hélices, c'étaient ces parties qu'il convenait de renforcer.

Figure 1 - Endroits endommagés des avions revenus



Source : McGeddon, 2016.

Un autre danger est celui où les relations causales sont inversées. Que penser de ce médecin qui prescrit un puissant neuroleptique à un patient mis en examen, de peur que la justice lui reproche de ne pas avoir vu la dangerosité de son patient, et qu'inversement, la justice s'appuie sur cette prescription pour prouver que le patient est dangereux ? Un algorithme mal conçu pourrait comprendre de travers le sens des relations causales.

Mais les modèles prédictifs en matière judiciaire ne sont pas que du côté des juges. Lors d'un accident corporel sur la route, la loi Badinter (du 5 juillet 1985) prévoit un droit à indemnisation pour toute victime d'un accident de la circulation dans lequel est impliqué un véhicule terrestre à moteur. Lorsque la société d'assurance du conducteur propose une indemnité, la victime fait une rapide analyse coût/bénéfice pour savoir s'il va au tribunal. Si elle ne construit pas formellement un modèle prédictif, elle tente de voir, à partir de quelques éléments à sa connaissance, les coûts de demander à un juge de trancher sur le montant de l'indemnité, et ses bénéfices (potentiels).

Autre point important, les juristes appellent ces modèles « prédictifs » des modèles « actuariels ». Or la première fonction des actuaires est, entre autres, d'actualiser, de calculer la valeur du temps. Et le temps judiciaire a des conséquences souvent désastreuses. En quoi une décision humaine, imparfaite, prise au bout de cinq ans de procédure serait meilleure qu'une décision automatique prise en quinze jours par une machine ? Nombre de personnes qui ont connu des procédures de plusieurs années, aboutissant à un non-lieu, rêvent de procédures accélérées. Car le « temps perdu » a une valeur, les actuaires le savent bien.

Que penser alors de cette efficacité des modèles algorithmiques ? La justice se doit d'être efficace, mais cette contrainte ne doit pas faire oublier l'objectif central qui est celui de rendre la justice. Que se passe-t-il si l'efficacité devient un objectif, pour ne pas dire le principal objectif ? Car c'est bien la question que posent les modèles prédictifs : quel est l'objectif que l'on cherche à maximiser ? Et comment le formule-t-on de manière simple ?

Aide à la décision ou justification d'une prise de décision

Aux États-Unis, nombre de juges se sont vu reprocher de motiver un jugement à l'aide d'outils d'aide à la décision, ce qui laisse planer un doute sur la fonction réelle de ces outils. L'idée était initialement d'apporter une aide. Récemment, plusieurs systèmes mis en place dans les années passées ont été remis en question. Par exemple en Australie, le STMP (Suspect Targeting Management Plan) proposait d'identifier si des préadolescents devaient être surveillés, ou pas. Ce modèle ressemble à s'y méprendre à n'importe quel modèle actuariel, c'est-à-dire un outil d'évaluation et de prédiction des risques, en se concentrant soit sur les récidivistes, soit sur les personnes suspectées de

commettre un futur crime. Or un rapport récent montrait que son utilisation n'avait eu « aucun impact observable sur la prévention du crime » (3). Parallèlement, aux États-Unis, l'outil Compas (Correctional Offender Management Profiling Alternative Sanctions) a été critiqué [Dressel et Farid, 2018] : « Les défenseurs de ces systèmes soutiennent que les données et l'apprentissage automatique avancé rendent ces analyses plus précises et moins biaisées que celles des humains. Cependant, nous montrons que le logiciel d'évaluation des risques Compas, largement utilisé, n'est pas plus précis ou juste que des prédictions faites par des personnes qui ont peu ou pas du tout d'expertise en matière de justice pénale ». En questionnant des personnes recrutées sur Internet, sans compétences en droit, il s'agissait de prévoir si des personnes allaient, ou pas, commettre un autre crime dans les deux ans à venir. Compas s'est trompé dans 34,8 % des cas, et les internautes dans 33 % des cas. Cela dit, on peut se demander ici ce que « se tromper » signifie. En l'occurrence, on ne mesure pas ici la récidive des personnes, mais la condamnation pour récidive des personnes. Et si les modèles (ou les gens) ne s'étaient pas trompés, mais que les juges, en revanche, oui ?

Prévoir, et se tromper

Et si un des soucis ne venait pas de ce que l'on demande à un outil prédictif ? Prévoir, c'est (fondamentalement) établir une probabilité pour un fait futur. Comme cela avait été rappelé dans un débat sur les sondages et les élections, est-ce qu'on peut dire qu'on se trompe si on annonce qu'un événement peut se produire avec 5 % de chance, et qu'il se produit effectivement ? Pour savoir si une technique de prévision est bonne, il faut collecter un ensemble de prévisions, et les comparer aux observations. C'est ce que font les météorologues depuis une quinzaine d'années, et qui a été formalisé par Gneiting *et al.* [2007]. Leur idée est qu'un ensemble de distributions prédictives est obtenu par un modèle $\{\hat{F}_t, \hat{F}_{t+1}, \hat{F}_{t+2}, \dots, \hat{F}_{t+h}\}$ et qu'il convient de comparer ces distributions aux observations $\{y_t, y_{t+1}, y_{t+2}, \dots, y_{t+h}\}$ – et non pas $\{\hat{y}_t, \hat{y}_{t+1}, \hat{y}_{t+2}, \dots, \hat{y}_{t+h}\}$. Il faut alors introduire une distance entre les distributions prédictives, et les observations. Dans un système physique, il est possible d'imaginer comprendre les différentes relations causales, et donc de prévoir. Mais dans les relations humaines (et la justice en est un exemple parfait), rien n'est aussi simple, aussi automatique que les lois de mécanique des fluides qui permettent de modéliser des phénomènes météorologiques.

Notes

1. En argot (slang) « wasted » *ne signifie pas « gaspillé » mais « ivre ».*

2. Décrit dans « In Your Face: China's all-seeing state », BBC, *10 décembre 2017. http://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state*

3. https://www.numerama.com/politique/300907-un-algorithme-teste-par-la-police-pour-anticiper-les-crimes-des-jeunes-inquiete-laustralie.html

Bibliographie

BINET J.-L., « La prévention médicale de la récidive chez les délinquants sexuels », Académie de médecine, 2010. *http://www.aihus.fr/prod/data/news/rapport_recidive_delinq_sex.pdf*

BOTSMAN R., *Who Can You Trust?: How Technology Brought Us Together – and Why It Could Drive Us Apart*, Portfolio Penguin, 2017.

CHARPENTIER A. ; SUIRE R., « Données et santé : valeurs, acteurs et enjeux », *Risques*, n° 107, septembre 2016.

CHARPENTIER A., « Les dérives du principe de précaution », *Risques*, n° 108, décembre 2016.

CHRISTIN A. ; ROSENBLAT A.; BOYD D., "Courts and Predictive Algorithms", Data & Civil Rights Conference, 2015. *http://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf*

DRESSEL J. ; FARID H., "The Accuracy, Fairness, and Limits of Predicting Recidivism", Science Advances, 2018. *http://advances.sciencemag.org/content/4/1/eaao5580.full*

FOUCAULT M., *Surveiller et punir. Naissance de la prison*. Gallimard, 1975.

GALEON D. ; BERGAN B., "China's 'Social Credit System' Will Rate How Valuable You Are as a Human". *futurism.com*, 2017. *https://futurism.com/china-social-credit-system-rate-human-value/*

GNEITING T. ; BALABDAOUI F. ; RAFTERY A., "Probabilistic Forecasts, Calibration and Sharpness". *Journal of the Royal Statistical Society* (JRRS-B), vol. 69, issue 2, 2007, pp. 243-268.

MANGEL M. ; SAMANIEGO F., « Abraham Wald's Work on Aircraft Survivability », *Journal of the American Statistical Association*, vol. 79, n° 386, 1984, pp. 259-267.

MCLANNAHAN B., "Being 'Wasted' on Facebook May Damage Your Credit Score", *Financial Times*, octobre 2015. *https://www.ft.com/content/d6daedee-706a-11e5-9b9e-690fdae72044*

SUPIOT A., *La gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Fayard, 2015.

TRUJILLO E., « La Chine met en place un système de notation de ses citoyens pour 2020 ». *Le Figaro*, 27 décembre 2017. *http://www.lefigaro.fr/secteur/high-tech/2017/12/27/32001-20171227ARTFIG00197-la-chine-met-en-place-un-systeme-de-notation-de-ses-citoyens-pour-2020.php*

La réforme de l'assurance incendie en Suisse : une perspective historique

Geoffroy Legentilhomme

Doctorant en histoire internationale (1)

Institut de hautes études internationales et de développement, Genève

L'histoire de l'assurance incendie en Suisse est chargée de controverses. Depuis la création des premiers établissements cantonaux – publics et en monopole – au début du XIXe siècle, la question de l'organisation industrielle optimale de la branche et du degré de concurrence qui devrait y régner fait l'objet d'intenses débats. Cet article retrace l'histoire bicentenaire de ces controverses, auxquelles furent mêlés d'influents groupes de pression aux intérêts parfois antagonistes.

En Suisse, l'assurance des bâtiments contre les incendies est exploitée par deux types de sociétés : d'une part, des établissements publics jouissant d'un monopole cantonal ; d'autre part, des sociétés privées (anonymes ou mutuelles), en concurrence. Sur les vingt-six cantons suisses, dix-neuf ont opté pour le premier modèle, les sept autres pour le second (Genève, Uri, Schwyz, Tessin, Appenzell-Rhodes intérieures, Valais et Obwald). La question controversée de la légitimité des monopoles publics d'assurance – et de leur performance relative – resurgit régulièrement à travers le pays. En juin dernier, par exemple, un débat sur le bien-fondé d'une motion en faveur de la libéralisation du secteur, introduite par une coalition de députés du centre (Vert'libéraux), de droite (UDC) et écologistes (Les Verts), a agité le Grand Conseil du Canton de Berne. La mise en concurrence, affirment les motionnaires bernois, combinée au maintien de l'obligation de s'assurer, améliorerait la qualité des services sans réduire la couverture des propriétaires immobiliers. Elle soulagerait également le canton du risque que ferait peser sur les finances publiques le déclenchement d'un sinistre majeur (2). La motion, rejetée par le Conseil exécutif, fut finalement retirée.

La naissance d'une controverse

La controverse, en vérité, n'est pas neuve. On en trouve des traces dès les premières décennies du XIXe siècle, période au cours de laquelle naquirent la plupart des établissements publics en opération aujourd'hui. Ces établissements mutualistes, émanation des autorités cantonales auréolées du prestige de l'indépendance retrouvée après la signature de l'Acte de médiation (1803), se heurtèrent à la critique de groupes de propriétaires immobiliers des villes, qui refusaient d'être contraints

de s'associer aux propriétaires des campagnes, dont les bâtiments couverts de chaume étaient davantage susceptibles de prendre feu. Entre les maisons des villes et les maisons des campagnes, lit-on dans un pamphlet dénonçant le projet de caisse cantonale, publié à Genève en 1820, « il y a des différences presque du tout au tout ; les bonnes maisons de la ville, celles qui ne courent presque aucun danger du feu, sont associées à des maisons appelées *brûlots* et à des dépendances de campagne (3). »

Mais des considérations d'utilité publique l'emportèrent dans la plupart des cantons : l'assurance d'État était conçue comme un instrument d'encouragement à l'industrie locale, par l'accroissement de la liquidité du marché immobilier, et surtout, par la stimulation du crédit hypothécaire. La justification offerte par le gouvernement du canton d'Argovie – le premier à fonder une caisse d'assurance incendie (1803) – est à cet égard représentative. L'assurance permettrait d'« élever les maisons et les bâtiments au rang d'hypothèque réelle, de consolider par là le crédit public et d'augmenter la richesse de chaque citoyen et par suite celle du canton tout entier (4). » Entre 1805 et 1821, quinze cantons suivirent l'exemple argovien et fondèrent des caisses publiques d'assurance contre l'incendie des bâtiments.

On reprocha à ces établissements, et au principe de l'assurance plus généralement, de décourager la prudence des propriétaires, et leur ardeur à lutter contre les incendies et à en prévenir le déclenchement. L'assurance mutuelle entre les propriétaires, affirme David Dunant en 1834, est « une prime à la fréquence des incendies, parce qu'elle tend à leur [les propriétaires] faire porter moins de surveillance sur l'état de leurs maisons, sur le choix des locataires, sur les métiers qu'ils exercent, sur l'accumulation des combustibles, sur leurs imprudences (5). » Pis encore, l'assurance, arguèrent ses détracteurs, menace de réduire la ferveur avec laquelle les citoyens portent secours aux incendiés, et, finalement, de corroder les vertus civiques et le sens du bien commun. C'est ce qu'exprime avec emphase l'historien genevois James Galiffe en 1820 : « Au lieu de ce zèle admirable qui fait courir jusqu'à nos dames les plus distinguées sur les lieux où le feu nous menace de quelque ravage, qui peut douter que même les jeunes gens les plus robustes n'en vinssent à dire : "Qu'est-ce que cela me fait ? Tant pis pour le Phoenix, tant pis pour telle ou telle compagnie d'assurance, dont la plaque déjà rougie par le feu enseigne que la maison est assurée et que le propriétaire n'y peut rien perdre (6)" ».

C'est, en d'autres termes l'argument classique de l'« aléa moral » que les adversaires de l'assurance mobilisèrent au début du XIXe siècle (sans certes que ce vocable fût employé). Pour éviter que l'assurance ne modifiât trop considérablement les incitations des propriétaires, et des citoyens en général, les législateurs jugèrent bon, dans la plupart des cantons, de limiter les indemnités à une fraction seulement de la perte subie. L'on cherchait, par cette clause de « coassurance », à établir un partage des risques, et à intéresser davantage le propriétaire au destin de son bâtiment. La même ambition présida à la volonté d'exclure les meubles du champ des choses assurées par les établissements cantonaux. Enfin, à l'objection que l'assurance détruirait les vertus civiques, l'on répondit qu'elle permettait au contraire, sous la forme mutuelle, d'intéresser chacun aux pertes de tous (la cotisation des membres variant en proportion des indemnités à verser annuellement) (7).

Des évolutions et des solutions

L'essor des compagnies à primes, et les premières réformes

À partir de la deuxième moitié du XIXe siècle, le développement des compagnies anonymes à primes fixes en Europe fit entrevoir une alternative aux caisses cantonales, et raviva la controverse. Après une brève et infructueuse tentative d'organiser l'assurance des bâtiments sur le principe de la gestion publique, le gouvernement du canton italianophone du Tessin

décida en 1854 de se tourner vers les compagnies étrangères à primes : une concession fut d'abord accordée à la Compagnie de Milan – en échange de quoi celle-ci s'engageait à verser au gouvernement un pourcentage des primes collectées –, puis la concurrence généralisée fut finalement établie dans la branche en 1859. Le gouvernement, affirme en novembre 1859 un rapport du Conseil d'État tessinois, « en assumant sur lui la charge d'assurer le canton, s'engagerait dans une entreprise très risquée, le rayon des opérations indispensables à son développement étant trop restreint (8). »

Dans d'autres cantons, en revanche, les événements politiques infléchirent l'évolution du secteur dans le sens de l'étatisation. L'une des premières motions déposées par Henri Druey, chef victorieux de la révolution radicale vaudoise de février 1845, visait à étendre le monopole public aux meubles – et non plus seulement aux immeubles. Cette mesure, impliquant de fait une évaluation de la richesse mobilière des citoyens par les agents de l'État, suscita l'opposition des conservateurs du canton, qui y virent une menace à la liberté individuelle, à l'inviolabilité de la sphère privée et à la sacralité du foyer (9). En dépit de ces protestations, le vœu des radicaux vaudois se réalisa en 1849.

Le vaste incendie qui dévasta la ville de Glaris en mai 1861, mettant à mal la caisse d'assurance de ce canton, accéléra le processus de réforme. Cet incendie, affirmèrent les adversaires du système public, révèle la fragilité de ces caisses cantonales, opérant sur un territoire étroit, et met en évidence la supériorité des compagnies à primes, dont les activités s'étendent sur plusieurs pays. À Genève, l'incendie de Glaris fournit un argument de poids au groupe de pression – déjà à l'œuvre depuis plusieurs années – favorable à la libéralisation. Il obtint gain de cause en 1864, lorsque le Grand Conseil vota, après de longs et laborieux débats, l'abolition de l'établissement cantonal et la libre entrée dans la branche (non sans que de grandes précautions eussent été prises pour que la transition ne nuisît pas aux intérêts des créanciers hypothécaires) (10). Les premières années de la décennie 1860 virent également naître les premières sociétés anonymes suisses d'assurance contre l'incendie des bâtiments, l'Helvetia (1861) et la Bâloise (1863).

Aucun autre canton ne poussa comme Genève la volonté réformiste jusqu'à l'abolition de l'établissement public. Mais afin de faire face aux risques associés à une catastrophe de grande ampleur, plusieurs méthodes – souvent empruntées aux sociétés anonymes – furent adoptées : le recours à la réassurance des risques agglomérés par des entreprises privées (comme à Neuchâtel, où la caisse publique signa en 1868 un accord de réassurance avec la Compagnie française du phénix (11), la répartition temporelle des risques par la création de fonds de réserves (solution adoptée par Berne en 1865, par exemple (12), abandon de la politique d'uniformité des primes au profit d'une politique de gradation adaptée au niveau de risque, lui-même fonction de la localisation et de la nature des immeubles (Bâle-Ville et Lucerne, par exemple, introduisirent la classification en 1869 (13). En somme, au cours de la deuxième moitié du XIXe siècle, les pratiques des caisses publiques tendaient à converger vers le modèle capitaliste des sociétés anonymes (14).

Un tournant idéologique

L'essor du socialisme en Suisse (le premier congrès de l'Association internationale des travailleurs se tint à Genève en septembre 1866, et les idées qui y furent échangées essaimèrent ailleurs en Suisse) donna une impulsion nouvelle à la thèse de l'assurance publique monopoliste. En 1878, la Société ouvrière cantonale de Glaris soumit au Landsgemeinde (15) une proposition visant à rendre publique et obligatoire l'assurance incendie des meubles – en vain. Au début des années 1890, la question fut également débattue à Zurich, Fribourg et Neuchâtel. La dimension idéologique du débat s'accentua. Les libéraux craignaient que la nationalisation de l'assurance constituât le cheval de Troie du socialisme d'État en Suisse, et qu'elle mît finalement en danger des libertés politiques et économiques plus fondamentales : « La nationalisation de l'assurance, lit-on dans un pamphlet de 1892,

se montre à nous, au point de vue social, comme un acheminement nouveau vers le socialisme d'État, qui annihile les initiatives particulières, qui avilit les caractères et qui prépare l'aplatissement général par le collectivisme. Politiquement, c'est la suppression d'une des libertés du citoyen. (…) Économiquement, c'est la fin d'industries et d'entreprises utiles, bienfaisantes et prospères (16) ».

Au reste, l'adoption d'une nouvelle constitution fédérale en 1874, dont l'article 31 spécifiait que « la liberté de commerce et d'industrie est garantie dans toute la Confédération », fournit un argument supplémentaire – d'ordre légal – au parti de la libéralisation : qu'est-ce que le monopole public de l'assurance, affirmèrent-ils en substance, sinon une atteinte à la liberté du commerce et de l'industrie (17) ?

Dans les dernières décennies du XIXe siècle, la défense des compagnies privées contre les projets de nationalisation fut prise par le Bureau fédéral des assurances, organe étatique fondé en 1885, et chargé de surveiller les activités des compagnies d'assurance étrangères et nationales opérant en Suisse. Ses directeurs – à travers les rapports que le Bureau devait faire paraître annuellement – s'employèrent à réfuter les objections élevées contre le capitalisme assuranciel (excès des frais administratifs et des dividendes versés aux actionnaires pour la plupart étrangers, procédures tracassières pour le règlement des indemnités…). « Le meilleur antidote contre une exagération des tarifs au profit des actionnaires, a été de tout temps la concurrence (18) » lit-on dans le rapport annuel de 1897. Naturellement, les partisans de la liberté assurancielle se réjouirent de disposer d'un si prestigieux allié, et ne se privèrent pas d'utiliser les rapports du Bureau fédéral, « ce juge compétent, et en même temps neutre et impartial (19) », comme un instrument de certification, validant scientifiquement la supériorité économique de la concurrence sur le monopole public.

En dépit de ces plaidoyers énergiques en faveur de la libéralisation, la cause du monopole public obtint quelques victoires significatives, notamment dans le demi-canton d'Unterwald-le-Bas (aujourd'hui Nidwald), où fut fondée en 1884 une caisse publique d'assurance immobilière, et surtout dans le canton des Grisons, qui fonda également une caisse en monopole, en 1907, après de longs débats, auxquels furent mêlées les compagnies anonymes, naturellement mécontentes de la décision issue de la votation populaire. Elles déposèrent un recours auprès du Tribunal fédéral afin de faire déclarer anticonstitutionnelle la loi grisonne, en vain (20).

Un apaisement relatif

Les controverses s'apaisèrent dans les décennies qui suivirent la Première Guerre mondiale, et, au cours du XXe siècle plus généralement, les projets de libéralisation ou de nationalisation se firent plus rares. L'enracinement du statu quo poussait les réformistes de tous bords à la résignation. Dans les cantons concurrentiels, la part de marché des compagnies étrangères – qui souffrirent des politiques économiques autarciques mises en place pendant la Première Guerre mondiale, et pour les compagnies allemandes, de l'hyperinflation de l'entre-deux-guerres – déclinait au bénéfice des compagnies suisses (21). Cette évolution privait progressivement les partisans du monopole de l'argument mercantiliste populaire, selon lequel le capitalisme assuranciel en Suisse enrichissait surtout les compagnies étrangères aux dépens d'institutions nationales. Quant aux établissements publics en place dans les cantons monopolistes, ils poursuivaient les politiques de modernisation entamées à la fin du siècle précédent. La réassurance se généralisait, tandis que l'importance accordée à la prévention s'accentuait (l'établissement de Fribourg, par exemple, adopta le contrôle des installations électriques en 1929 (22)). En outre, les établissements cantonaux adoptèrent dans l'entre-deux-guerres les méthodes de rationalisation de l'organisation travail en vogue dans le secteur privé (diffusion de la machine à écrire, puis de la machine à carte perforée (23)). Sur un plan plus strictement actuariel, la répartition temporelle des risques par accumulation de réserves se diffusait, de sorte que ces établissements cessèrent progressivement d'être de simples centres de redistribution, et

purent élaborer des politiques d'investissement, contribuant, de fait, au développement des institutions financières nationales et au processus d'accumulation du capital. Ces évolutions privèrent peu à peu les critiques de l'assurance publique du recours à l'accusation – fréquente – d'archaïsme.

Si les débats s'apaisèrent, ils ne cessèrent toutefois pas définitivement. En 1949, à Genève, une coalition, formée de députés du Parti socialiste et du Parti du travail, tenta une nouvelle fois de rétablir l'assurance cantonale en monopole (après l'échec en 1908 d'un projet de loi constitutionnelle, rejeté à 80 % en votation populaire), abolie en 1864. La coalition échoua à obtenir une majorité au Grand Conseil (24). Quelques tentatives furent faites dans le même sens dans le canton alpin du Valais (en 1930 et en 1969, par exemple) – pourtant relativement épargné par les controverses au siècle précédent – mais aucune n'aboutit (25). Le statu quo, en somme, était solidement établi, et, nulle part, les poussées réformistes n'ébranlèrent les arrangements en place : au XXe siècle, aucun canton ne jugea bon de changer de système.

Intégration européenne et libéralisation des services

Cependant, la question de l'organisation industrielle du secteur de l'assurance incendie resurgit avec force à la fin du XXe siècle, à une époque où le projet d'intégration économique européenne parvenait à maturité et où la libéralisation des services avait le vent en poupe dans la plupart des pays industrialisés. En Allemagne, la transposition de la troisième directive européenne sur l'assurance non vie (92/49/CEE, 18 juin 1992) – qui établit les conditions du marché unique dans la branche –, conduisit à l'abolition des établissements publics régionaux d'assurance incendie. La Suisse, quant à elle, signa en 1989 un accord avec la Communauté européenne garantissant la liberté d'établissement et d'exercice des institutions d'assurance non vie. Si cet accord ne remit pas directement en cause l'existence des monopoles publics cantonaux, il ouvrit néanmoins une brèche, dans laquelle s'engouffrèrent les assureurs privés. En 1992, Max Gretener, directeur de l'Association suisse des assureurs de choses, en appela à la libéralisation de l'assurance incendie des bâtiments par la suppression des monopoles cantonaux ; suppression, qui, note-t-il, « s'avère inéluctable, si l'on prend au sérieux les efforts de libéralisation et de revitalisation de l'économie suisse et l'harmonisation en toute autonomie des systèmes juridiques et économiques de notre pays, afin qu'ils coïncident de plus en plus avec la législation de la Communauté européenne (26). »

Naturellement, les établissements cantonaux ne demeurèrent pas passifs face à cette charge. En 1994, l'Association des établissements cantonaux d'assurance incendie chargea l'économiste Thomas von Ungern-Sternberg (Université de Lausanne) de conduire une expertise sur les performances relatives des caisses cantonales et des sociétés privées ; son rapport, publié en 1994, établit que les conclusions classiques de la théorie économique enseignant la supériorité de la concurrence sur le monopole ne s'appliquent pas à l'industrie de l'assurance incendie, caractérisée par d'importantes défaillances de marché. Ce rapport donna lieu l'année suivante à une contre-expertise de Bernd Schips (École polytechnique fédérale de Zurich), mandatée par les assureurs privés, qui elle-même suscita une contre-contre-expertise la même année (27). Mais la campagne des assureurs privés finit par s'enliser, et le dualisme du secteur de l'assurance incendie se maintint.

Conclusion

L'histoire de l'assurance incendie en Suisse est, en somme, jalonnée de controverses. La question de l'organisation industrielle optimale de la branche et du degré de concurrence qui devrait y régner – question qui, au premier abord, n'évoque que des enjeux techniques et « de surface » – renvoie en réalité à une problématique politique et morale plus profonde : l'emploi de

moyens légaux contraignant les citoyens – en l'occurrence propriétaires immobiliers – à l'achat d'un service particulier, auprès d'un fournisseur particulier, relève-t-il du rôle légitime de l'État ou constitue-t-il une atteinte à la liberté individuelle ? C'est en somme l'éternelle question de la philosophie politique que ces controverses soulèvent. Il est donc fort à parier que le débat bernois de juin 2017 ne soit pas le dernier, et que la réforme de l'assurance incendie continue à agiter les parlements cantonaux.

Notes

1. geoffroy.legentilhomme@graduateinstitute.ch

2. Grand Conseil du canton de Berne, session de juin 2017, « Abolition du monopole de l'Assurance immobilière », motion n° 188-2016.

3. J.-A. Martin-Sales., « Le projet de garantie réciproque contre les incendies », 1820, p. 1 (italiques dans l'original).

4. Cité par le Rapport du Bureau fédéral des assurances sur les entreprises privées d'assurances en Suisse en 1892, Schmid, Franke & Co, 1894, p. LXVIII.

5. D. Dunant, Incendies de Genève : préservatifs et notice historique*, Genève, 1834, p. 10.*

6. J. Galiffe, Lettre à M. ***, Membre du Conseil représentatif, sur le projet de faire assurer les maisons de Genève contre l'incendie*, Genève, 1820, p. 5.*

7. Voir par exemple J.-P. Bridel, Rapport au Conseil représentatif, Genève, 1820, p. 6.

8. Cité par F. Ballinari, Il Ticcino e la Lotta al fuoco*, Armando Dadò, 2017, p. 125.*

9. L. Marti, De l'assurance à la prise en charge complète du risque*, ECA, 2011, p. 60.*

10. Archives d'État de Genève, Mémorial du Grand Conseil*, 1864, pp. 2386-2612.*

11. La Chambre d'assurance de la république et du canton de Neuchâtel*, 1810 - 1910, Paul Seiler, p. 86.*

12. P. Alglave, « L'État et la province assureur, en Suisse et dans les pays scandinaves », thèse de doctorat, Université de Paris, 1901, p. 196.

13. L. Rossi, « L'assurance cantonale contre l'incendie en Suisse », thèse de doctorat, Université de Neuchâtel, 1920, p. 38.

14. Rapport du Bureau fédéral des assurances sur les entreprises privées d'assurances en Suisse en 1890, Schmid, Franke & Co, 1892, p. LXII.

15. Communauté rurale ou assemblée du pays.

16. Ignotius, L'assurance mobilière par l'État*, Attinger, 1892, pp. 219-220.*

17. Gazette de Lausanne*, 23 janvier 1890.*

18. Rapport du Bureau fédéral des assurances sur les entreprises privées d'assurances en Suisse en 1897, Schmid, Franke & Co, 1899, p. LX.

19. Assurance par l'État ou Assurances par les compagnies ? Réponse impartiale à cette question par un juge compétent et neutre*, Attinger, 1892, p. 3.*

20. L. Rossi, « L'Assurance cantonale contre l'incendie en Suisse », thèse de doctorat, Université de Neuchâtel, pp. 86-87.

21. M. Lengwiler, « Switzerland: insurance and the need to export », in Borscheid P. et Viggo Haueter N., eds., World Insurance: The Evolution of a Global Risk Network*, Oxford University Press, 2012, pp. 152-155.*

22. La Liberté*, « L'Établissement cantonal d'assurance des bâtiments fête le 150e anniversaire de sa fondation », 11 septembre 1962.*

23. L. Marti, De l'assurance à la prise en charge complète du risque*, ECA, 2011, p. 103.*

24. Archives d'État de Genève, Mémorial du Grand Conseil*, 1949, pp. 1346-1353 et 1477-1495.*

25. Voir Le nouvelliste valaisan*, 27 décembre 1930 et 25 novembre 1969.*

26. M. Gretener, « Wettbewerb in der Gebäudeversicherung/ Concurrence en assurance des bâtiments », Schweizerische Versicherungszeitschrift*, vol. 61, n° 9-10, 1993, pp. 217-225.*

27. Sur le débat opposant Thomas von Ungern-Sternberg à Bernd Schips, voir Kirchgassner G., « Idéologie et information en matière de conseils politiques : quelques remarques et un exemple réel », Cahier de recherches économiques, *n° 9624, Université de Lausanne, 1996, pp. 1-40.*

Les débats de *Risques*

Sécurité routière
comment progresser

Le 10 janvier 2018 Risques *a organisé un débat sur la sécurité routière. Étaient réunis pour en évoquer les enjeux : Emmanuel Barbe, délégué interministériel à la Sécurité routière, Anne Lavaud, déléguée générale de l'association Prévention routière et Patrick Jacquot, président de l'association Attitude Prévention.*

Le débat était animé par Arnaud Chneiweiss et Pierre-Charles Pradier, membres du Comité éditorial de Risques.

Risques : Hier soir, le Comité interministériel à la Sécurité routière (CISR) a lancé le plan « Sauvons plus de vies sur nos routes ». Nous avons globalement le sentiment qu'il existe un plancher de verre sous lequel le nombre de tués sur la route ne peut descendre, compte tenu de la croissance de la circulation. Est-ce une illusion ? Pouvez-vous nous expliquer les grandes mesures prises pour casser ce plancher ?

Emmanuel Barbe : Le point que vous soulevez sur le plancher de verre est important car il renvoie à la façon dont nous mesurons notre performance. Les médias se concentrent, et nous aussi, sur le nombre de morts tous les ans, mais il ne faut pas oublier que c'est un cortège de blessés, avec pour ratio un mort pour sept blessés, ce qui, pour la collectivité, en termes de souffrance et de dépenses médicales, est extrêmement élevé.

Depuis de nombreuses années, nous assistons à une baisse du nombre de morts en valeur absolue, alors que la courbe du trafic augmente. Depuis 2014, la courbe des morts est remontée, tandis que la courbe des kilomètres parcourus a plutôt stagné. Le bilan 2016 indique seize morts de plus qu'en 2015 (une légère hausse). En revanche, le ratio par rapport au kilométrage parcouru marque, en 2016, le même niveau de risque que celui de 2013. Mais en même temps, si vous prenez ce ratio (nombre de morts par kilomètres parcourus) et si vous le rapportez à d'autres pays, vous vous rendez compte que si nous voulions imiter l'Allemagne, nous devrions être à 2 700 morts (non pas en nombre de morts par million d'habitants, mais en nombre de morts par kilomètres parcourus). Si nous voulions être comme la Suède, nous devrions être à 2 000 morts par an, alors que nous sommes à 3 477 morts en 2016.

Il ne faut pas oublier que depuis 2015 des mesures importantes ont été prises : abaissement du taux d'alcool autorisé à 0,2 gramme d'alcool par litre de sang pour les conducteurs novices (ce qui implique

en pratique zéro verre d'alcool car dès le premier verre ce seuil peut être dépassé) ; la décision de l'externalisation de la conduite des voitures-radars, qui va permettre de contrôler la vitesse partout ; ensuite, une loi très importante, celle qui oblige le titulaire du certificat d'immatriculation personne morale à désigner, sous peine d'amende assez lourde, le conducteur flashé au volant d'un véhicule. On estime que 75 % des entreprises désignent aujourd'hui le conducteur, contre 10 ou 12 % avant cette loi. Par ailleurs, le taux de réitération d'infraction des véhicules dont le propriétaire est une personne morale va vraisemblablement baisser très fortement.

Malgré cela, nous sommes encore très en dessous de nos meilleurs voisins. C'est pour cela que le Premier ministre a décidé de mesures d'une grande amplitude.

Indépendamment de l'expérimentation menée par Bernard Cazeneuve il y a deux ans, qui ne portait que sur 80 kilomètres, une expérimentation sur les baisses de vitesse avait été faite en 1997, sur 1 600 kilomètres : dix-huit mois après, on baissait les vitesses. On constate surtout un précédent sur tout le territoire et sur ce réseau, c'est 2002, où les premiers radars automatiques sont installés. Ils ont un effet performatif extraordinaire. Tout le monde se dit qu'il y a des radars partout, une sorte de psychose naît, et tout le monde ralentit. En trois ans, la vitesse baisse : sur le réseau concerné par la mesure 80 km/h, la baisse est de 7 km/heure, et la mortalité de 37 % ! L'idée, grâce à un dispositif radar efficace et une règle que spontanément 60 à 65 % des conducteurs respectent, est de faire baisser la vitesse moyenne ; cela produit un effet mécanique sur le nombre d'accidents en raison des règles de la cinétique. Celui qui roule moins vite va plus facilement éviter quelqu'un qui a trop bu par exemple. C'est cela qui se met en œuvre quand on applique des règles à ce niveau. Pour mémoire, près de 43 millions de véhicules roulent en France ; c'est donc un risque global qui baisse. Dans deux ans, le Premier ministre dressera le bilan de cette mesure. Le succès dépendra du niveau d'adhésion des citoyens ; c'est pour cela que nous allons communiquer massivement dans l'ensemble des médias, y compris les réseaux sociaux, pour que la mesure soit à la fois comprise, acceptée le plus possible, mais aussi pour que personne n'ignore que le 1er juillet la vitesse passe à 80 km/h, de façon à avoir un effet mécanique de respect de la règle. Sans les radars.

Cette mesure est très importante. Il va de soi qu'elle sera accompagnée, dans les deux ans à venir, de l'externalisation de l'ensemble des voitures-radars sur l'ensemble des routes du réseau. Cela finira par se savoir et il y aura aussi un respect de la vitesse inspiré par la crainte du radar. Par ailleurs, notre « stratégie radar » aboutira à terme à substituer les radars fixes actuels par des radars aux capacités accrues (par exemple pouvant identifier une personne utilisant son téléphone) dont le nombre sera le même mais qui seront logés de manière aléatoire au sein de près de 10 000 cabines installées au bord des routes (systèmes de leurre) ; on ne saura donc jamais si la cabine est active ou pas, et les cabines actives alterneront. Notre objectif est de faire ralentir, ce n'est pas de flasher plus. Le Premier ministre s'est engagé à ce que toutes les recettes liées à l'abaissement à 80 km/h, et donc aux inévitables flashs supplémentaires (du moins juste après le passage à 80 km/h, ce surcroît de flashs ayant vocation à diminuer), soient affectées à l'amélioration des conditions dans les hôpitaux des victimes de la route. C'est une réponse à cette accusation, totalement infondée, qu'une telle mesure n'a pas pour motif la sécurité routière mais le gain d'argent. C'est une mesure de rupture, pour essayer d'atteindre le niveau des pays de même niveau économique.

Le plan concerne aussi l'alcool, qui reste un problème majeur dans notre pays. Les mesures comportent plusieurs aspects : favoriser l'utilisation des éthylotests, en essayant de développer le plus possible la vente d'éthylotests dans les magasins où sont vendus 90 % des boissons. L'idée serait d'avoir des éthylotests en vente à côté des alcools. Nous allons aussi chercher à développer considérablement l'éthylotest anti-démarrage (EAD), qui a d'abord été prévu dans un cadre judiciaire, avec la loi LOPPSI (1) en 2009, puis dans un cadre préfectoral, actuellement expérimenté

dans quatre départements avant son extension à tout le pays. Ce système a de grandes vertus pour éviter la récidive. Il y a deux mesures dans le CISR. Désormais, quand une personne sera contrôlée pour une alcoolémie délictuelle (supérieure à 0,8 gramme) son permis lui sera retiré et le préfet émettra un arrêté de suspension du permis de conduire jusqu'au jugement. Mais, si son taux reste en deçà de certaines limites et que le conducteur n'est pas récidiviste, cet arrêté pourra autoriser la personne à conduire à la condition qu'elle équipe son véhicule d'un éthylotest anti-démarrage. Nous avons maintenant 158 installateurs qualifiés, bientôt trois fabricants sur le marché, et surtout la promesse d'un marché véritable, et donc l'espoir d'une baisse des prix substantielle. Grâce à cette mesure, nous pouvons espérer permettre à des gens de conduire en sécurité pour la société, mais sans être déclassés parce qu'ils perdent leur emploi. Nous espérons en poser beaucoup, que cela fasse baisser les prix, et que cela sécurise les routes.

En matière d'alcool, il y a une deuxième mesure importante : permettre aux forces de l'ordre, à leur demande, de suspendre temporairement la localisation de leur contrôle d'alcoolémie. Ce dispositif a été discuté avec les opérateurs des services de navigation. Les forces de l'ordre leur communiqueront le périmètre des zones pour lesquelles leur localisation ne devra pas être répercutée. Naturellement, ce système pourra également être utilisé pour les contrôles de stupéfiants ou de lutte contre la criminalité, mais pas pour ceux de vitesse : les radars sont en nombre suffisant.

Une autre mesure vise à sanctionner plus sévèrement l'utilisation du téléphone à la main en voiture. Pour éviter de priver un trop grand nombre de personnes de leur permis de conduire, nous avons retenu un élément discriminant : seul celui qui tient son téléphone à la main et commet une autre infraction (tourner sans clignotant, déboîter sans avertir) pourra se voir retirer son permis de conduire. C'est assez brutal mais je pense que c'est à la hauteur de l'enjeu, car nous sommes face à un problème majeur. Dans les recrudescences de morts en ville, notamment de piétons, on peut penser que le téléphone joue un rôle assez fort.

Dernier point, mais pas le moins important : une mesure de mobilisation générale autour de la prévention et de la sécurité routière. Nous voulons toucher tous les secteurs où il y a des collectivités humaines : les écoles, les universités, les entreprises, l'État avec dans chaque ministère un haut fonctionnaire sécurité routière chargé de mettre en œuvre une politique de sécurité routière pour les fonctionnaires de l'État. J'espère que les collectivités territoriales, du moins celles d'une certaine taille, nous imiteront. Nous voulons aussi sensibiliser les acteurs de l'assurance dans le monde du travail. Ils ont intérêt à faire de la prévention pour faire baisser le risque qu'ils indemnisent. Or le risque routier est le premier risque professionnel.

Voilà toute une série de mesures. Il y en a d'autres qui font que nous espérons que ce plan programmatique ambitieux, sur cinq ans, produira des effets.

Anne Lavaud : Nous avons un ratio de cinquante-quatre tués par million d'habitants. C'est une moyenne. Ce qui est plus intéressant ce sont les ratios par département ; cela nous permet de nous comparer avec d'autres pays. L'Île-de-France, par exemple, avec environ vingt tués par million d'habitants a un ratio comparable à celui du Danemark, souvent cité en exemple. Dans certains départements ruraux, ce ratio monte à cent tués par million d'habitants. La mesure de 90 à 80 km/h est un élément de réponse à cette disparité. En effet, ce sont dans ces départements que l'on trouve le plus de routes bidirectionnelles concernées par cette mesure. Cette disparité est intéressante à pointer parce qu'elle est contre-intuitive. Instinctivement, on va considérer que ce sont dans les lieux où il y a plus de monde, où se croisent les voitures, les vélos, les piétons, les engins de déplacement personnel (hoverboards, trottinettes) que l'on est en grand danger. La réalité est inverse. Nous sommes plus en danger dans le Cantal, dans l'Orne...

La prévention est donc essentielle, et les assureurs, qui étaient à nos côtés à la création de l'association

Prévention routière, doivent en être convaincus – comme ils le sont dans d'autres domaines de la prévention – et rester mobilisés pour ne pas accepter ce plancher de verre en matière de sécurité routière.

Patrick Jacquot : Le Comité des constructeurs français d'automobiles (CCFA) a publié en décembre dernier son étude annuelle qui est une référence en matière de transport routier global. En 2016, il observe pour la troisième année consécutive une croissance du transport intérieur de voyageurs par habitant : + 1,9 %, principalement liée à l'augmentation de la mobilité, favorisée ces dernières années par la baisse du coût des carburants et les mesures prises par le président Macron en faveur de la circulation des bus et des cars. On assiste à une plus grande utilisation de la voiture particulière, dont la circulation a augmenté de 2,8 % en 2016. C'est un élément à prendre en compte. Pour en revenir au plan, il repose sur trois axes : mobiliser, protéger et anticiper. Mobiliser est l'axe majeur. Il faut en conséquence, si l'on veut mobiliser les citoyens, s'adresser notamment à ceux qui sont responsables, qui, de bonne foi, peuvent commettre des impairs, leur fournir des éléments de contexte qui viendront renforcer la nécessité d'une vigilance accrue de leur part.

Anne Lavaud : On pourrait ajouter qu'il y a toujours eu une corrélation entre la croissance économique et l'accidentalité. De toute évidence, on repart dans une séquence de croissance économique, ce qui est une très bonne chose, mais ce qui doit nous obliger à davantage de vigilance par rapport à l'accidentalité routière.

Emmanuel Barbe : Nous sommes d'accord sur ce point. Parallèlement on constate que le débat sur la sécurité routière est perturbé par certaines personnes opposées à plus de mesures de sécurité routière, pour lesquelles le seuil auquel nous sommes parvenus est suffisant. Elles le répètent depuis toujours, quel que soit le nombre d'accidents, de blessés et de morts. Pour parvenir à un résultat comparable à celui des démocraties les plus avancées, nous devons changer notre méthode de mesure. C'est pour cela que nous avons passé des marchés publics pour essayer d'obtenir le nombre de kilomètres parcourus quasiment en temps réel. Dans six mois, grâce aux marchés que nous avons passés, nous devrions obtenir le kilométrage parcouru du mois précédent. Cela va nous permettre de mieux mesurer les résultats, par la connaissance du nombre de tués et du nombre réel de kilomètres parcourus, sur le modèle de l'industrie aéronautique. Nous pourrons avoir une base de comparaison (car nous avons acheté des données cinq ans en arrière), afin d'avoir une mesure très exacte des évolutions. En effet, on pourrait croire par moment que cela va bien, alors que cela va très mal. Et vice versa.

Cela nous permettra aussi de nous comparer plus finement avec les pays ayant les meilleurs résultats. Je ne vois pas pourquoi les Suédois arrivent à l'équivalent de ce qui serait 2 000 morts pour nous. Ils ont 1 700 morts d'avance sur nous ; ce n'est pas rien. Cela s'accumule tous les ans. Pourquoi serions-nous moins civilisés qu'eux ?

Patrick Jacquot : Il faut aussi prendre en compte l'évolution des usages et le renouvellement générationnel. On voit bien aujourd'hui le succès du covoiturage, qui renforce l'utilisation de véhicules individuels. Les données du CCFA indiquent que le transport augmente en nombre de véhicules mais que parallèlement les émissions de CO_2 diminuent. Cela répond au souhait des jeunes générations, tournées vers le développement durable. Ce sont elles qui seront demain les plus concernées par les messages et les décisions qui seront prises.

Pour en revenir à la mesure du 80 km/h, précisons que l'association Attitude Prévention, dont la signature est « Donnons de l'assurance à la vie », ne peut que saluer l'efficacité d'une telle mesure – qui permettra potentiellement d'épargner 200 à 400 vies –, et l'évaluation qui doit en être faite. Cependant, pour être acceptée cette mesure doit être comprise. Il est donc essentiel que notre association, qui s'adresse aux assurés – collectivement ou individuellement –, relaye les messages des pouvoirs publics sur la base de motifs argumentés ; afin qu'ils les acceptent, se les

approprient et fassent évoluer leurs comportements. Dans l'évolution des comportements, j'inclus notamment l'utilisation des téléphones portables, que ce soit en voiture, à vélo ou à moto. C'est un axe de progrès important.

Risques : Les assureurs ont deux formes de rôle social : un rôle social microéconomique, ce sont eux qui mettent en œuvre le principe du « pollueur-payeur » sur la route, en faisant payer aux mauvais conducteurs le prix de leur mauvaise conduite. N'ont-ils pas aussi un rôle social macroéconomique, qui consiste à jouer un rôle de lobby auprès des pouvoirs publics ? Ils jouent ce rôle en finançant la prévention routière. Ils doivent en être fiers pour cette raison. Y a-t-il eu une histoire du rôle des assureurs dans les grandes campagnes de lutte contre la mortalité routière ?

Anne Lavaud : Ce que vous dites est important. Il faut que les assureurs continuent à jouer ce rôle. Ils ont été présents auprès de l'association Prévention routière dès 1949, convaincus de l'efficacité des actions de prévention auprès d'un plus grand nombre, auprès des jeunes, auprès des enfants essentiellement, par rapport à ce risque. J'ai la conviction que toutes les actions menées conjointement par les assureurs et par l'association Prévention routière ont eu une efficacité, et que cette efficacité a eu un retour sur investissement sur le long terme. Oui, il faut que les assureurs soient partie prenante et disent qu'ils sont des préventeurs, et que l'assurance, c'est aussi de la prévention, pour eux-mêmes, et pour leurs assurés. À ce titre, et pour continuer à agir au plus près des risques, nous avons créé, en partenariat avec Attitude Prévention, un nouvel observatoire de la mobilité et des risques routiers, en utilisant les techniques du *big data*, de manière à pouvoir mesurer le delta entre la réalité des comportements et le déclaratif des Français.

Notre association travaille également sur la voiture autonome qui est une de nos préoccupations majeures. L'espèce de pensée magique, qui consiste à dire qu'avec la voiture autonome il n'y aura plus d'accidents parce que 90 % des risques seraient dus à des facteurs humains, circule dans le monde entier. C'est absurde. Il va y avoir d'autres risques qui seront fondamentalement humains. Il va falloir les identifier, pour non seulement pouvoir construire (et les assureurs ont leur rôle à jouer) les produits assuranciels pour cette nouvelle masse assurable, mais aussi pour trouver les actions de prévention par rapport à ces risques nouveaux qui ne vont pas tarder à arriver.

Risques : Allons-nous, avec la voiture connectée, vers une amélioration de la sinistralité ? A-t-on déjà des éléments chiffrés ou est-il encore trop tôt ?

Emmanuel Barbe : Avec la Direction générale des entreprises et le ministère de la Transition écologique et solidaire, nous sommes en train d'élaborer une « stratégie nationale du véhicule autonome » pour réfléchir à son développement – c'est d'abord un projet industriel – et à ses impacts. Nous la soumettons actuellement à la consultation publique. Le véhicule autonome apporte d'ores et déjà le développement et l'abaissement du prix des aides à la conduite (Adas [2]), ce qui est bénéfique pour la sécurité routière. Par exemple, notamment en ville, le freinage automatique est incontestablement une très bonne chose. Demain vous aurez des voitures équipées de manière à ne pas déboîter si une moto, un piéton ou un cycliste arrivent dans l'angle mort. Mais ce type de véhicules restera longtemps minoritaire. Il restera à renouveler le stock, ce qui prendra du temps, le coût de ces voitures étant élevé. Par ailleurs, une partie, au demeurant vulnérable, des usagers, ne s'inscrira pas dans l'élan : les deux-roues, les vélos, les piétons.

Patrick Jacquot : Le fait que les véhicules, même s'ils ne sont pas autonomes, soient équipés d'un système permettant de repérer les deux-roues (qu'ils soient motorisés ou non), est un réel progrès. On sait que le conducteur, de bonne foi, ne les voit pas forcément parce qu'il ne s'attend pas à les avoir dans son champ visuel. Et cela s'aggrave car les deux-roues sont noyés dans ce qu'on appelle un bruit visuel, duquel il leur est impossible d'émerger (feux de jour à LED, allumage des feux de croisement même si les fameuses LED sont allumées). Si demain des systèmes

signalent les vélos, les motos, comme ils signalent déjà le franchissement de la ligne ou permettent le freinage automatique, le très vieux message revendiqué par les conducteurs de deux-roues, qu'a minima les autres usagers, dans d'autres véhicules, anticipent en mettant leur clignotant et en regardant dans leur rétroviseur... fera des progrès.

Anne Lavaud : Par rapport aux aides à la conduite, ces fameux « adas », un sujet nous préoccupe, en tant qu'association de prévention du risque, c'est l'absence d'harmonisation entre les différents constructeurs. Une même aide à la conduite ne va pas réagir de la même manière sur tous les véhicules. C'est parfois si déstabilisant que cela crée un nouveau facteur de risque. Mais je sais que des travaux d'harmonisation sont engagés. De la même manière, nous avons beaucoup de témoignages de gens qui débranchent tous ces « adas » parce qu'ils n'arrivent pas à s'y habituer. La conduite, c'est quand même la force de l'habitude, beaucoup de réflexes, même si c'est l'un des actes les plus compliqués demandé à l'être humain. Conduire requiert une attention proche de celle d'un sportif de haut niveau, ou d'un musicien chevronné. Si le changement d'instrument ou de voiture occasionne une perte de réflexe, on risque la fausse note en musique, mais l'accident en voiture ! D'où l'importance qu'il y ait un travail d'harmonisation de ces « adas ». Une commission du Comité national de la Sécurité routière (CNSR) travaille sur ce sujet ; c'est un point de vigilance.

Risques : Pour conclure, y a-t-il un domaine d'action sur lequel vous souhaitez insister ?

Anne Lavaud : Nous avons bien sûr besoin de l'aide du secteur de l'assurance car vous avez la capacité de mettre un prix sur un risque, donc de lui donner une valeur qui est difficile à appréhender sur une notion aussi abstraite. Et nous avons également besoin des médias pour diffuser plus massivement un message positif de la prévention du risque routier, tout en redoublant de pédagogie afin de permettre aux journalistes de battre en brèche les nombreux arguments infondés que portent ceux qui prônent la vitesse, par exemple.

Patrick Jacquot : Aujourd'hui, Attitude Prévention couvre trois champs : prévention des risques routiers, prévention des risques santé, accidents de la vie courante. Nous nous adressons aux mêmes citoyens, aux mêmes usagers. Au sein de l'association, nous sommes quelques-uns à penser qu'il faut peut-être décloisonner, et ne plus raisonner par type de risque puisqu'on s'adresse finalement à un citoyen qui, à différentes périodes de la journée ou de la vie, est soumis à des risques différents. C'est la même culture de la prévention en général qu'il convient de développer dans notre pays.

Emmanuel Barbe : En juillet, nous baissons la vitesse. On passera à 80 km/h sur 400 000 kilomètres de route. Le résultat de la fin de l'année sera conditionné au nombre de gens qui vont respecter cette mesure. Très clairement, mécaniquement, cela signifie une baisse potentielle du nombre de sinistres. Il pourrait donc être souhaitable que les assureurs – et je leur en serais très reconnaissant – relayent cette mesure en faisant preuve d'une pédagogie active vis-à-vis de leurs assurés.

Notes

1. Loi d'orientation et de programmation pour la performance de la sécurité intérieure.

2. Advanced driver-assistance systems.

Actualité de la Fondation du risque

La chute du taux d'actionnaires français depuis la crise

Luc Arrondel
CNRS et PSE

André Masson
CNRS, EHESS et PSE

*L'épargne des ménages français est abondante, voire surabondante (*savings glut*), s'élevant à près de 16 % du revenu disponible brut (RDB) – seuls les Allemands font mieux. Elle serait toutefois mal orientée. Elle serait tout d'abord trop immobilière. Mais l'épargne financière de notre pays, de près de 6 % du RDB (mais 8 % en Allemagne), reste supérieure à la moyenne de la zone euro (5 %). Le débat porte en fait sur la structure de cette épargne financière, jugée trop prudente : en France, la part des produits d'épargne réglementés (Livret A par exemple) et des fonds en euros, fiscalement avantagés, dépasse la moitié du patrimoine financier brut en 2016 (contre 40 % seulement dix ans plus tôt), alors que les titres et les contrats en unités de compte font 35 % de ce patrimoine (contre 45 % en 2006). Comment expliquer la faible détention d'actions par nos compatriotes ? Quelles solutions pour y remédier ?*

Les raisons d'une détention d'actions limitée

Les raisons communes invoquées par les professionnels français peuvent être résumés en six points. Les deux premiers concernent la demande des ménages :

- manque de culture et d'éducation financière, d'appétence au risque, voire de « désir d'épargne » financière, longue et risquée ;

- manque de confiance des ménages français, qu'elle soit générale (pessimisme sur leur situation personnelle ou le contexte économique), ou spécifique (dans leur banque).

Les deux points suivants ont trait aux contraintes fiscales et réglementaires :

- une fiscalité sur les produits actions lourde en France (hors contrats en unités de compte), qui pâtit encore d'une imposition moins élevée des placements immobiliers et des avantages accordés à l'épargne réglementée ;

- une réglementation prudentielle de plus en plus contraignante (Solvabilité II, fin 2009, pour l'assurance vie ; Bâle III, fin 2010, pour les banques).

Les deux derniers portent sur l'offre de placements :

- inadaptation de l'offre de conseil bancaire ou financier (manque de transparence et d'information sur les produits offerts, connaissance lacunaire ou biaisée du client) ;

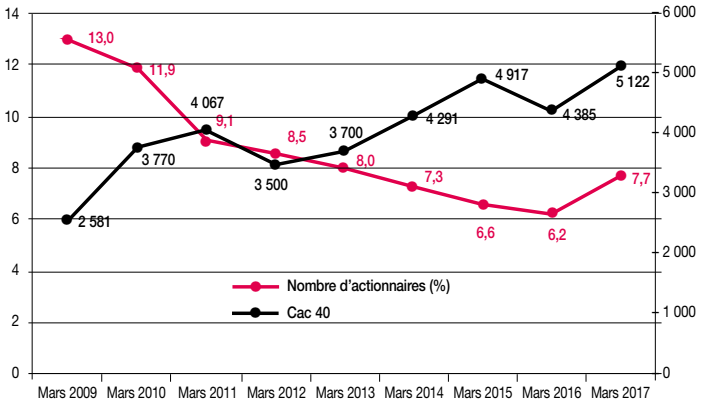
- innovation produits trop timorée, qu'il faudrait développer autour du concept « d'épargne-projet », adaptée aux différentes phases de leur cycle de vie (logement, professionnel, préparation de la retraite – fonds de pension à la française –, dépendance, voire transmission).

Ce discours peut être critiqué [Arrondel et Masson, 2018], tel le premier point : les comparaisons internationales, avec des mesures certes imparfaites, montrent que l'aversion au risque n'est en moyenne pas plus élevée en France qu'aux États-Unis et que notre pays se situe honorablement en termes d'éducation financière (avec un niveau inférieur à celui de l'Allemagne ou des Pays-Bas, mais supérieur à celui des États-Unis, du Japon, de l'Italie ou de la Suède). De fait, la détention directe d'actions reste supérieure en France à celle de nombre de ses voisins continentaux (Allemagne, Italie, Espagne, Pays-Bas). Mais surtout, la crise de 2008 constitue une véritable mise à l'épreuve de ce discours.

La crise depuis 2008, observatoire dramatique mais riche en informations

Le graphique 1 ci-dessous, tiré de l'enquête Kantar TNS-Sofia, résume la seule information d'ensemble sur la détention d'actions au-delà de 2014 : il révèle pour la France une chute à la fois sensible et régulière chez les individus du taux d'actionnaires directs, de 13,8 % en décembre 2008, à 6,2 % en mars 2016 (au cours d'une période où le CAC 40 a plutôt eu tendance à augmenter), mais également une rupture de tendance après, avec un rebond en mars 2017 au niveau de mars 2014.

Graphique 1 - Évolution du nombre d'actionnaires individuels depuis la crise (détention directe)



Source : Kantar TNS-Sofia 2017.

Les données transversales des enquêtes Patrimoine de l'Insee en 2004, 2010 et 2014, et les données de notre enquête PATER (1), avec une forte dimension de panel, effectuées de mai 2007 à décembre 2014 (*cf. infra*), toutes deux représentatives de la population française, permettent d'en connaître beaucoup plus sur la période concernée. Leurs conclusions convergentes montrent que la baisse régulière du taux d'actionnaires concerne aussi bien la détention directe qu'indirecte (FCP-actions), les particuliers et les ménages, et impacte tous les âges depuis 2004 : cette baisse uniforme selon l'âge, ainsi que le maintien d'une épargne financière élevée, ne permettent pas d'attribuer la diminution de l'actionnariat par un report de l'épargne sur l'immobilier (2). Seuls échappent à cette baisse de la détention les contrats en unités de compte. Leur diffusion globale, inchangée entre fin 2010 et fin 2014, ne peut cependant expliquer la baisse de la détention des autres produits actions.

L'alourdissement de la fiscalité actions depuis 2008, surtout fin 2012 (passage au taux marginal sur les revenus du capital comme sur les revenus du travail), aurait en revanche joué un rôle dans cette baisse – les contrats en unités de compte y auraient échappé du fait du traitement fiscal préférentiel dont ils ont continué à bénéficier (3). L'instauration prochaine d'une *flat tax* limitée (30 %) sur les revenus du capital, sur le mode scandinave, pourrait donc nuire à la diffusion des contrats en unités de compte au bénéfice d'autres produits actions.

Cette explication fiscale doit cependant être relativisée : la baisse sensible de la détention directe comme indirecte d'actions se retrouve entre 2010 et 2014 en Allemagne, en Italie, en Espagne et aux Pays-Bas, soit dans des pays qui n'ont pas connu le même « choc fiscal » de 2008 à 2012 que la France. En revanche, les nouvelles règles prudentielles pour les sociétés d'assurance vie (fin 2009) et les banques (fin 2010) ont impacté l'ensemble des pays et pourraient avoir joué sur l'offre de placements risqués.

Les explications avancées jusqu'ici sont utiles mais laisseront le lecteur sur sa faim. Pour les professionnels notamment, la chute du nombre d'actionnaires pendant la crise serait encore imputable à une hausse de l'aversion pour le risque et une perte de confiance dans leur banque des épargnants. Qu'en est-il vraiment ?

Les enseignements du panel PATER sur le comportement des épargnants dans la crise

Du côté de la demande, les comportements de moins en moins risqués des ménages depuis la crise peuvent être attribués, selon la théorie économique, à trois types de facteurs : les préférences (moindre tolérance au risque) ; les ressources disponibles (plus faibles ou plus risquées) ; les anticipations de prix d'actifs, *i.e.* des anticipations boursières plus pessimistes, ou une perte de confiance (générale ou spécifique). Or les remèdes adaptés à la baisse de l'actionnariat varient beaucoup selon le poids respectif de ces trois catégories de facteurs.

Les quatre vagues du panel PATER (en mai 2007, juin 2009, fin 2011 et fin 2014) recueillent sur des échantillons de près de 4 000 ménages des données comparables à celles des enquêtes Patrimoine de l'Insee, mais interrogent aussi les individus sur leurs préférences à l'égard du risque et du temps à l'aide d'une méthode originale de *scoring*, leurs anticipations boursières, professionnelles (revenu, chômage) et autres à un horizon de cinq ans, leur degré de confiance dans leur banque, leur niveau d'éducation financière, leurs intentions d'investissement (plus ou moins risqué), etc.

Les dates des quatre vagues ont été bien choisies puisqu'elles encadrent les deux chocs de la crise (Lehman Brothers en 2008, dettes souveraines à l'été 2011). La dimension panel se traduit par le fait que deux vagues successives ont au moins 2 000 ménages en commun et 807 d'entre eux ont participé aux quatre vagues. Les scores indicateurs de préférences, qui s'avèrent bien supérieurs aux mesures usuelles, agrègent les réponses à un grand nombre de questions diverses (une soixantaine dans le cas du risque) : les

mêmes questions ont été posées aux différentes vagues pour une comparaison optimale.

Résumons les principaux résultats obtenus [Arrondel et Masson, 2017a et b].

• La psyché des épargnants n'a pas changé pendant la crise : leur aversion (ou plutôt leur attitude générale) face au risque est restée globalement stable sur la période. Les deux chocs de 2008 et 2011 n'ont pas eu d'incidence statistique sur les préférences (les variations individuelles pouvant être assimilées à des bruits blancs). En revanche, la tolérance au risque diminue (modérément) avec l'âge pour les mêmes ménages au cours du temps.

• Les anticipations de la prime de risque sur le marché boursier, déjà basses en 2007, ont sensiblement diminué en 2009, et plus encore fin 2011 ; elles remontent un peu après (fin 2014).

• La confiance spécifique dans sa banque qui avait diminué entre 2009 et 2011 est revenue fortement fin 2014. (4)

• Parallèlement, les intentions d'investissement exprimées par les ménages, de moins en moins en faveur d'actifs risqués entre 2007 et 2011, se redressent un peu fin 2014.

• Parmi les facteurs susceptibles d'influer (économétriquement) sur la variation de la détention d'actions au cours de la période, les variations individuelles de préférence sont sans effet et le fait d'avoir été « touché par la crise » a un effet (négatif) limité ; la dégradation des anticipations boursières et la perte de confiance dans sa banque sont les principaux facteurs explicatifs de la baisse de la détention d'actions du côté de la demande des ménages.

Si les épargnants sont restés stoïques pendant la crise jusqu'à la fin de 2014, leurs perceptions du monde ont en revanche changé, contribuant à expliquer leur désaffection pour les actions. Reste une « énigme » du côté de la demande : les anticipations boursières, le degré de confiance dans sa banque, mais aussi les intentions d'investissement en placements risqués remontent à la fin 2014 : autrement dit, les facteurs a priori les plus susceptibles d'expliquer la baisse de la détention d'actions jusqu'à la fin 2012 jouent plutôt dans le sens contraire après cette date… mais la chute du taux d'actionnaires continue jusqu'en 2017.

Au-delà d'un « effet de retard » dans les réponses comportementales, la solution est sans doute à rechercher du côté de l'offre. Selon les visites mystères de l'Autorité des marchés financiers (AMF), l'offre de conseil bancaire s'est dégradée entre 2012 et 2015, en particulier sur des notions clés du questionnaire client (projet, horizon de placement, charges…). Quelles qu'en soient les raisons – fiscalité dissuasive, formation économique insuffisante des conseillers financiers, rigidité de certaines directives européennes liées à ces conseils, etc. –, cette offre est de moins en moins tournée vers les produits actions (détention directe et même indirecte), à l'exception notable des contrats en unités de compte dont l'offre est plébiscitée.

Recommandations en faveur d'une relance de l'actionnariat

Souvent évoquée, la promotion de l'éducation financière n'aurait que des effets à très long terme : elle devrait être menée très tôt, dès la plus tendre enfance, et viserait à produire un « épargnant nouveau », moins averse au risque et à horizon plus long, mieux informé et désireux d'épargner. Reste que les épargnants des pays les plus lettrés financièrement (Allemagne, Pays-Bas) ne sont pas plus souvent actionnaires que les autres.

Des mesures plus efficaces à moyen terme porteraient sur l'amélioration de l'offre de conseil bancaire ou financier, afin d'inciter les conseillers financiers à trouver une meilleure adéquation entre l'offre de produits et le profil des épargnants : construction de questionnaires harmonisés de meilleure qualité,

notamment pour mesurer l'appétence au risque des épargnants ; formation continue des conseillers, certifiée par les régulateurs, etc.

Les réformes fiscales en cours en France – taxation forfaitaire des revenus du capital, abolition de l'impôt sur la fortune (ISF) et création de l'impôt sur la fortune immobilière (IFI) – devraient améliorer l'attractivité des produits actions, du moins si elles apparaissent crédibles et s'inscrire sur le long terme. La discussion précédente montre cependant qu'une fiscalité discriminante n'est qu'une cause parmi d'autres de la désaffection des épargnants vis-à-vis du marché boursier – la fiscalité moins lourde sur les actions d'autres pays ne se traduit pas toujours par un taux d'actionnaires plus important. Et les mesures fiscales à venir pourraient déprimer la demande de contrats en unités de compte. S'il est donc difficile de juger ex ante de l'ampleur des effets d'une réduction de la fiscalité sur les produits actions, on peut néanmoins présumer qu'elle sera moins importante sur leur taux de détention que sur les montants investis par les actionnaires (aisés).

Le point clé concernerait plutôt, selon notre étude, les anticipations et le degré de confiance des ménages à l'égard de la bourse et des intermédiaires financiers. S'il est resté stoïque pendant la crise, l'épargnant juge aussi que le monde autour de lui est devenu plus chaotique et indéchiffrable : se considérant globalement plus exposé au risque, il privilégie de ce fait des placements plus prudents, selon un processus avéré de « substitution des risques ». Le remède consisterait ici à créer un choc de confiance global, économique et social, par des politiques macroéconomiques (de stabilisation) instaurant un environnement plus stable et moins incertain, des réformes conduisant à assurer la fiabilité et éclairer l'avenir de notre protection sociale, ou encore des innovations financières garantissant une transformation mieux adaptée de l'épargne financière en investissements productifs, gérés dans des fonds dédiés par des investisseurs responsables. Ce choc multidimensionnel permettrait à l'épargnant d'évoluer dans un monde moins ambigu, davantage propice à des prises de risque financières.

Cette étude a montré tout l'intérêt de disposer, en plus des données de l'Insee, des informations uniques fournies par le panel PATER pour comprendre les comportements financiers des épargnants français depuis la crise. Elle révèle en même temps un manque : ces données PATER s'arrêtent fin 2014, nous laissant dans une relative ignorance sur la période qui suit. On sait par exemple que les flux d'achat en unités de compte sont globalement à la hausse depuis, mais on ne connaît pas leur répartition ni les causes réelles de cette hausse. Une nouvelle vague PATER serait ici indispensable, qui offrirait par ailleurs un point de référence précis pour apprécier de manière fiable les effets sur la demande d'actions des prochaines réformes fiscales sur le capital, et permettrait également de mieux comprendre le retour (modéré) des Français à la bourse après mars 2016.

Notes

1. Patrimoine et préférences face au temps et au risque.

2. Cette diminution de l'actionnariat ne s'explique pas davantage, au moins après 2012, par la libéralisation du Livret A (rendue effective au début de 2009) : la forte croissance des dépôts s'arrête en effet à la fin de 2012.

3. Les contrats en unités de compte auraient encore bénéficié de leur « accouplement » aux contrats en euros dans les offres bancaires, mais aussi d'un conseil bancaire polarisé sur ces placements (cf. infra).

4. Le degré de confiance pour résoudre la crise dans les hommes politiques comme celui dans les économistes ont, eux, continûment baissé au cours de la période. L'indicateur de confiance générale (données CVS), au plus bas mi-2008 puis en mars 2013, présente depuis une tendance ascendante marquée.

Bibliographie

ARRONDEL L. ; MASSON A., « La chute du taux d'actionnaires français depuis la crise : une énigme ? », (bilingue français-anglais), *Opinions & Débats*, n° 17, Institut Louis Bachelier, 2017a.

ARRONDEL L. ET A. MASSON, "Why Does Household Demand for Shares Decline during the Crisis?", (bilingue français-anglais), *Economics and Statistics*, n° 494-495-496, 2017b, pp. 155-178.

ARRONDEL L. ; MASSON A., « Épargne et croissance : le rôle des ménages en question », *in* Aglietta (Ed.), *Transformer le régime de croissance*, Caisse des dépôts, 2018, à paraître.

Livres

François Meunier

Comprendre et évaluer les entreprises du numérique

Eyrolles, octobre 2017, 208 pages

Pour bien apprécier la pertinence et les qualités de ce livre, il suffit de vouloir appliquer les techniques « classiques » d'évaluation des entreprises (celles enseignées en classe, dans les cours de gestion financière) pour constater combien elles sont inadéquates, donc inutiles, dans le domaine du numérique. La technique comptable et financière la plus « rationnelle » – la technique DCF (*discounted cash-flow*) – consiste en une série de fractions dont les numérateurs sont des indicateurs de rentabilité (dividendes, profits nets, Ebidta, etc.) et les dénominateurs des taux d'actualisation. Comment remplir un numérateur lorsque la rentabilité est nulle, voire quand le chiffre d'affaires est inexistant, pire lorsque les pertes sont abyssales pendant les premières années, donc quand elles coûtent cher en valeur actualisée ? Côté dénominateur, les difficultés conceptuelles ne sont pas moindres. Quel taux d'intérêt appliquer lorsque les risques de perte sont élevés ? Surtout comment appliquer la formule dite de Gordon et Shapiro où le dénominateur est la différence entre un taux d'intérêt jugé pertinent et le taux de croissance anticipé de l'entreprise, différence telle que ce dénominateur est négatif ? Pour un épargnant prudent mais cherchant tout de même à optimiser son plan d'épargne retraite en achetant des actions cotées, ces difficultés d'évaluation sont rédhibitoires. De fait, pour se financer les entreprises du numérique ont depuis longtemps déserté les bourses au profit (au sens propre comme au figuré) des « *venture capitalists* » et autres apporteurs de capitaux dans le non coté, acceptant le risque pour ne pas dire le recherchant. L'autre méthode d'évaluation, la comparaison avec des entreprises similaires, n'est pas non plus opératoire. Tout simplement parce qu'il n'y a pas de comparaison, même dans le numérique ! Comment comparer avec l'un des Gafa l'ancien géant de l'informatique IBM qui – avant de se réduire à n'être qu'une société de services en informatique comme d'autres – fabriquait ses machines, avait son système d'exploitation, son langage machine et ses logiciels et vendait le tout via ses ingénieurs commerciaux ? De même, comment comparer *leboncoin.fr* avec un journal de petites annonces ou *booking.com* avec une agence de voyage ? Ce n'est pas tout à fait par hasard si « disruption » est devenu le mot fétiche qualifiant les entreprises du numérique.

Partant de cette impossibilité de raisonner classiquement, François Meunier – praticien de la finance qu'il enseigne à l'Ensae Paris Tech –, analyse les pratiques pour le moins disruptives des évaluateurs. Par exemple, il montre sur des cas concrets que l'évaluation dans le secteur numérique se fait à rebours des techniques classiques. Au lieu de commencer par évaluer les cash-flows, depuis les plus proches jusqu'au plus éloignés, puis d'ajouter in fine la plus-value éventuelle, comme le ferait un investisseur dans l'immobilier qui évalue les loyers puis la plus-value sur la revente du bien, les *venture capitalists* commencent par la valeur finale estimée, laquelle peut être gigantesque, pour remonter vers le présent en évaluant les pertes et les apports de capitaux nécessaires avant d'arriver à la valeur finale. Évidemment, les déchets sont nombreux. Combien de « licornes » potentielles sont mortes pour une ou deux réussies ? La clé pour comprendre ces pratiques nouvelles tient dans le pouvoir de monopole qu'une « licorne » a dès lors qu'elle a réussi. Les Gafa en donnent plusieurs illustrations. Google, Amazon, Facebook, Apple, mais aussi Uber, Le Bon coin, Booking et bien d'autres n'ont pratiquement pas de concurrents, du moins jusqu'à ce qu'une nouvelle disruption ne les déloge, comme ce fut le cas avec Nokia. Malgré sa position enviable dans la téléphonie mobile, Nokia n'a pas vu la rupture fatale de l'écran tactile développé par Apple, qui transformait le vulgaire téléphone en un véritable ordinateur portable. Ajoutons que ce pouvoir de monopole est d'autant plus inexpugnable que les Gafa ont accumulé suffisamment de bénéfices non distribués pour faire face

à la concurrence, par exemple en la rachetant.

Mais l'intérêt du livre va bien au-delà de son titre. C'est toute l'analyse économique du numérique qu'il remet en cause, la renouvelant. Dans vingt-et-un encadrés insérés dans le texte, l'auteur aborde toutes les disruptions en cours ou prévisibles. Citons : n° 1 la *blokchain*, un exemple de numérisation aux conséquences très profondes ; n° 2 le marketing, le *big data* et la réduction du surplus du consommateur… ; n° 19 empiler le cash dans le bilan, une forme d'assurance contre le risque technologique ; n° 20 la Bourse et les entreprises technologiques ; enfin le n° 21, qui inquiète beaucoup le secteur bancaire : la numérisation et le potentiel de la pure banque de dépôt.

Un livre stimulant et indispensable pour comprendre l'économie actuelle.

Par Daniel Zajdenweber

Robert J. Gordon

The Rise and Fall of American Growth: The US Standard of Living since the Civil War

Princeton University Press, 2016, 762 pages

Pour rendre hommage à un ouvrage aussi savant et bien construit, deux phrases s'imposent : un travail monumental et une lecture qui incite à la réflexion sur un sujet en toile de fond plutôt délaissé, celui de la politique industrielle ! Et pourtant il faut souligner que les perspectives et conclusions que l'auteur nous propose dans les derniers chapitres de son livre sont loin d'être optimistes et encore moins indiscutables, au contraire.

Avec une vie entière consacrée à l'étude de l'investissement et de la productivité, Gordon nous offre une fresque complète de la croissance et de la productivité aux États-Unis sur un siècle et demi. Extrêmement précis et équilibré dans ses jugements, du moins dans les deux premiers tiers de son livre, avec un appareillage statistique facile à comprendre même par les profanes, il fait œuvre de pédagogie dans un domaine également délaissé, celui de l'histoire économique.

Son ouvrage se présente en trois parties et dix-huit chapitres. La première partie, avec huit chapitres qui s'étendent de 1870 à 1940, constitue la moitié de l'ouvrage. C'est la plus intéressante en termes de détail et profondeur dans les analyses qui lient inventions et mesure de la productivité. Elle traite en effet des grandes inventions de cette période et de leur diffusion rapide et massive : de l'électricité aux infrastructures sanitaires, en passant par la motorisation de l'économie et des individus, jusqu'aux nouveaux moyens d'information et de communication, dont de nouvelles formes de divertissement avec l'arrivée de la radio et de la télévision. L'auteur montre comment les dérivés de ces inventions ont, pendant un demi-siècle, radicalement transformé les conditions d'existence et la vie elle-même de la population des États-Unis, à la maison et au travail, dans les villes comme dans les zones rurales. Pour faire pendant au chapitre 2 qui ouvre cette partie, avec un état des lieux minutieux des conditions de vie et de travail, très dures, autour de 1870, il « clôture » cette période, en 1940, en montrant comment toutes ces inventions et innovations ont créé de nouveaux modes de consommation, et amélioré considérablement la qualité et la durée de vie, moyennant entre autres la massification de prestations jusque-là inédites en matière de santé et d'éducation. Si de nouveaux risques surgissent pendant cette période, de nouveaux métiers et activités permettant leur gestion accompagnent l'émergence de cette nouvelle culture étroitement liée à la deuxième révolution industrielle, notamment via l'extension rapide des assurances vie, santé et dommages aux biens, des crédits à la consommation et au logement… Tout ceci sur fond de hausse de la productivité et de la croissance, telle que mesurée par Gordon.

La deuxième partie, chapitres 10 à 15, de 1940 à 2015, traite de l'âge d'or, qui caractérise la croissance des années de post-guerre, du moins selon l'auteur, jusqu'aux années 1970, pour laisser place ensuite à des signes d'essoufflement de la productivité moyenne ce dernier tiers de siècle. Selon Gordon, les gains de productivité des périodes précédentes commencent à s'estomper après les premières décennies de la troisième révolution industrielle, celle de l'informatique et d'Internet. Sujet récurrent de cette partie, et également de la suivante, pour l'auteur, le rythme et l'intensité des innovations en cours sont loin d'atteindre l'impact sur les conditions de vie qu'elles ont eu entre 1900 et 1970. C'est ce dernier sujet que lui permet d'assurer la transition vers la troisième partie (composée de trois chapitres) dans laquelle il analyse les facteurs qui expliquent le ralentissement de la productivité et, de manière obsessionnelle, dresse des perspectives pas toujours très optimistes concernant ce que certains appellent la stagnation séculaire de la productivité et de la croissance. Comparativement aux innovations nées entre 1900 et 1970, il fait preuve d'autant de pessimisme que d'impatience concernant l'impact relatif des nouvelles technologies et de leur vitesse de diffusion.

Si l'ouvrage en soi est monumental, la qualité et la profondeur des analyses diminuent au fur à mesure qu'il approche de notre époque. Comme souvent dans le domaine des sciences sociales – et surtout lorsqu'il s'agit d'évaluer des phénomènes historiques proches –, les analyses ont tendance à refléter beaucoup plus les opinions de l'auteur qu'une vision objective des phénomènes observés. De ce fait, et point critique de fond, on est quelque peu déçu par la légèreté qui prédomine dans les analyses des cinq derniers

chapitres. Elle contraste avec la profondeur du travail réalisé pour la période 1870-1940, et les trente années qui suivent. On dirait que l'auteur n'avait pas assez de données pour mener à bien des analyses plus poussées – ce qui semble peu probable –, ou qu'il n'a pas pu ou su prendre suffisamment de recul pour juger des phénomènes contemporains. Ainsi, ses analyses sur les trente à quarante dernières années apparaissent brouillées par des considérations qui semblent chercher beaucoup plus à valider sa thèse centrale, c'est-à-dire la propension à la stagnation de la productivité et de la croissance, que les faits en eux-mêmes. Certaines considérations politiques ou idéologiques, relatives notamment au discours très en vogue sur les inégalités croissantes, qui transparaissent du texte, apportent une dose de subjectivité à cette partie de l'ouvrage qui, dans son approche fondée sur de nombreuses statistiques, se veut très objective. Ceci se reflète dans les jugements qu'il porte, sans pour autant les expliquer et encore moins les justifier, sur la relativement faible vitesse de diffusion et l'impact mitigé qu'il attribue aux innovations de ces dernières décennies comparativement à celles de la deuxième révolution industrielle. Par ailleurs, s'il les traite, Gordon ne prête qu'une faible attention au potentiel de croissance découlant des innovations liées à la révolution numérique, par exemple celles ayant lieu dans les sciences médicales (dont la génétique et de manière générale les nanotechnologies), et plus précisément celles liées aux applications en rapide développement dans les domaines de la médecine personnalisée, du traitement des maladies rares aujourd'hui difficilement guérissables (dont la maladie d'Alzheimer) ou, en matière de cancer, dans le domaine des traitements alternatifs visant à éliminer, voire atténuer les effets secondaires de la chimiothérapie.

Quant au contexte de notre époque, caractérisée par une troisième révolution industrielle dont la vitesse de diffusion ralentit aux États-Unis, pays de l'innovation par excellence, Gordon, qui est loin d'être un adepte du libéralisme, met en évidence que des régulations de plus en plus contraignantes freinent les innovations, leur diffusion et leur impact, ce qui explique en partie le phénomène de ralentissement dans les secteurs de pointe de l'économie de demain, notamment dans le domaine des biotechnologies et des autorisations concernant la mise sur le marché de nouvelles molécules.

Enfin, si les analyses de Gordon portent exclusivement sur l'économie américaine, dans un contexte de globalisation rapide des économies, ses résultats doivent être relativisés en raison de l'existence d'au moins deux phénomènes concomitants, et positifs, à ne pas négliger. D'une part, la forte croissance de la productivité ce dernier tiers de siècle dans les économies émergentes, phénomène dont on peut difficilement faire aujourd'hui abstraction. D'autre part, en dépit du ralentissement constaté de la productivité moyenne, celle des entreprises globalisées (*frontier firm* dans le jargon de l'OCDE), majoritairement d'origine nord-américaines et européennes, est non seulement très robuste, mais elle creuse l'écart vis-à-vis de celle des *non-frontier firms* ou entreprises à portée locale, par nature moins soumises à la concurrence. Ceci explique les raisons pour lesquelles des technologies ne se diffusent qu'inégalement ou pas assez rapidement.

À cet égard, question considérée jusqu'à récemment comme passéiste ou même démodée, cet état de fait remet à l'ordre du jour le besoin pressant de la mise en place de politiques industrielles dignes de ce nom, qui favorisent l'innovation et une meilleure diffusion de la productivité en affinant les incitations des entreprises à adopter des technologies nouvelles et en promouvant un environnement de marché qui réaffecte les ressources aux entreprises les plus productives. Il en va de l'avenir de la productivité et de la résilience de nos systèmes économiques et sociaux, si chers à Robert J. Gordon !

Par Carlos Pardo
Économiste

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

VENTE AU NUMÉRO - BULLETIN D'ABONNEMENT

		Prix France
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
101	Cybersécurité, *terra incognita*. Survivre à des taux d'intérêt historiquement bas.	39,00
102	Les nouvelles addictions. *Compliance* : entre raison et déresponsabilisation.	40,00
103	Le choc du *big data* dans l'assurance. L'e-santé est-elle une révolution ?	40,00
104	Risques de la croissance urbaine. Les multiples facettes du défi climatique.	40,00
105	L'assurance automobile face aux chocs du futur. Terrorisme et assurance.	41,00
106	Assurer la culture ? Gérer la multiplicité des risques pays.	41,00
107	Matières premières : richesse ou malédiction ? Montée des risques et populisme.	41,00
108	Les risques du vivant. Les ruptures dans la mondialisation, quel impact sur l'assurance ?	41,00
109	Le risque climatique est-il assurable ? La protection des données personnelles des individus.	42,00
110	Le choc démographique dans l'entreprise. Comment rendre liquide le patrimoine immobilier des ménages.	42,00
111	L'assurance contribue-t-elle au développement de l'industrie spatiale ? Le rôle insoupçonné de la capitalisation dans les retraites en France.	42,00
112	Heurs et malheurs de la *supply chain*. Brexit : *soft* ou *hard* ?	42,00

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. +33 (0)1 40 22 06 67
Courriel : info@seddita.com
www.seddita.com

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 (0)1 40 22 06 67 - Courriel : info@seddita.com

❑ Abonnement annuel (4 numéros) FRANCE 148 € EXPORT 168 €*

❑ 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

Notes

Notes

Notes