L'informatique et sa sécurité. Le souci de la fragilité technique

Jérôme Denis

L'informatique et sa sécurité
Le souci de la fragilité technique*

Jérôme DENIS

LTCI (UMR 5141) CNRS - TELECOM ParisTech
Département Sciences Économiques et Sociales
denis@telecom-paristech.fr

Résumé

Cet article propose d'explorer les politiques de sécurité informatique en entreprises en insistant sur deux dimensions : la définition des risques sur laquelle elles s'appuient et l'hybridité sociotechnique que revendiquent certains prescripteurs. Ces dimensions donnent à voir un mode d'existence des technologies qui contraste fortement avec les modèles constructivistes, généralement centrés sur les processus de stabilisation. Proches des domaines de l'entretien et de la maintenance, les politiques ordinaires de sécurité installent une manière distribuée de traiter les technologies qui fait de l'instabilité et de la vulnérabilité des propriétés intrinsèques. Elles s'apparentent ainsi à un *care* des objets, cherchant à faire de la fragilité technique un souci partagé.

Mots clés

Sécurité informatique - Prescription - Fragilité - Construction sociale des technologies - post-ANT

Denis, J. 2012. L'informatique et sa sécurité. Le souci de la fragilité technique. *Réseaux*, vol. 30 (171), p. 161-187

* Mes remerciements à David Pontille qui partage une grande partie des questions développées ici et avec qui la discussion est permanente. Je remercie aussi vivement les intervenants de la journée d'études qui a donné lieu à ce numéro spécial pour leurs remarques précieuses.

Les conditions du développement considérable des technologies électroniques de communication dans les entreprises peuvent sembler contradictoires. En parallèle de l'enthousiasme avec lequel certains vantent les améliorations multiples qu'elles sont censées apporter à l'efficacité et la productivité, un discours plus inquiétant a vu le jour, qui souligne les problèmes que ces mêmes outils soulèvent en termes sécuritaires. Si les nouvelles technologies sont puissantes, elles sont aussi terriblement vulnérables. Et s'il est vivement conseillé de les adopter et d'en user abondamment, il est aussi de plus en plus recommandé de s'en méfier et de prendre de nombreuses précautions pour renforcer une sécurité que la nature même des dispositifs semble fragiliser. De nombreux acteurs, y compris au sein des médias généralistes, mettent ainsi en avant ce qui semble être le prix à payer pour l'entrée dans la société de l'information. Virus, intrusions, pannes, sont les dangers ordinaires d'un monde où la communication, la circulation des informations, la constitution et le partage de connaissances apparaissent dans le même temps facilités et menacés.

Ce paradoxe n'en serait pas un si les deux mouvements étaient portés par des acteurs spécifiques dans des mondes différents. On se trouverait alors face à la forme classique des controverses qui ont fait la richesse des travaux de sociologie et d'histoire des techniques[1]. Il y a bien sûr de nombreux débats dans le domaine de l'informatique professionnelle, y compris à propos des pratiques de sécurité, mais les propos sécuritaires qui soulignent à grand renfort d'alertes ou de campagnes de sensibilisation les dangers de l'informatique ou ceux du Web et des communications en ligne sont en grande partie tenus, notamment dans les entreprises, par les porte-parole mêmes de ces technologies. La vulnérabilité des outils informatiques n'est pas décrite au service d'un projet critique. Elle apparaît au contraire comme une propriété même de la technique ; propriété qui ne doit pas remettre en cause la progression des nouvelles technologies, mais qu'il faut prendre en compte pour assurer la solidité d'activités, notamment professionnelles, au sein desquelles l'informatique en réseau tient désormais une place centrale.

Aujourd'hui, la sécurité informatique dans les entreprises est un domaine légitime, même si les frontières de ce qu'elle recouvre restent floues (Denis, 2009a). Elle fait en tout cas figure d'évidence sur le plan général. Si les méthodes qui lui sont dédiées et le périmètre qui lui est réservé sont évidemment discutés et débattus, personne en revanche ne défend l'idée qu'il ne faudrait pas sécuriser les échanges, les machines ou les réseaux de communication. Pourtant, hormis quelques rares exceptions (notamment : Boullier, et al. 2007 ; Chateauraynaud et Trabal, 2007), les politiques sécuritaires restent largement ignorées par les chercheurs qui s'intéressent à la place des technologies de communication dans les organisations. Et si l'on connaît les grandes lignes des principaux discours médiatiques qui décrivent les enjeux de la sécurité informatique, on sait mal comment, au jour le jour, le souci sécuritaire s'actualise dans les entreprises, quelles formes il prend. On ne sait pas non plus ce qu'il fait des technologies et de leurs usagers, alors même qu'il est une des sources importantes d'encadrement des pratiques professionnelles.

Cela est d'autant plus regrettable qu'il me semble que les politiques ordinaires de sécurité informatique ne représentent pas seulement un cas supplémentaire à ajouter à l'étude de la place des technologies dans les organisations, mais qu'elles soulèvent des enjeux théoriques importants, tant du côté des sciences de l'organisation que de celui de la sociologie des techniques. Si l'on accepte de les prendre en considération, plutôt que de leur opposer systématiquement une posture critique établie *a priori*, les discours et les dispositifs sécuritaires permettent en effet de laisser de côté pour un temps l'intérêt pour le seul caractère résistant et structurant des dispositifs sociotechniques. Ils invitent analyser la *fragilité* comme un mode d'existence complémentaire, si ce n'est principal, de certaines technologies.

Pour aborder cette double question, de la sécurité et de la fragilité techniques, je propose de m'appuyer sur une enquête par entretiens, effectuée auprès d'entreprises de tailles et de secteurs

[1] Il est impossible de citer les innombrables recherches qui se sont nourries de l'analyse des controverses. Pour un point général, on pourra se reporter à Bijker et Law (1992), Latour (1993) ou encore le récent recueil de textes sur la sociologie de la traduction (Akrich, Callon & Latour, 2006).

d'activité très différents[2]. Je procèderai en quatre étapes. Tout d'abord, j'exposerai rapidement les enjeux théoriques d'une telle exploration, d'une part en la situant dans un débat récent en sociologie des techniques et d'autre part en la rattachant aux quelques travaux qui se sont préoccupés de fragilité matérielle. Ensuite, je décrirai successivement deux dimensions essentielles de cette étude : le type de fragilité que la définition des principaux risques informatiques fait émerger, et la division du travail spécifique qu'elle implique au sein des entreprises, entre techniciens prescripteurs et usagers ; division qui donne à voir le véritable investissement des premiers dans des assemblages hybrides au sein desquels les seconds sont appelés, parfois contre leur gré, à jouer un rôle important. Enfin, je rattacherai les politiques de sécurité informatique au cadre plus général du travail de maintenance (Denis, & Pontille, 2010a) en montrant en quoi celui-ci déplace un modèle de la sociologie des techniques largement focalisé sur les dynamiques d'innovation et invite à étudier plus sérieusement des formes de rapport aux objets techniques comparables au *care* (Denis, & Pontille, 2011).

L'angle mort de la fragilité technique

Depuis quelques années, plusieurs travaux, notamment en sociologie de l'organisation et en gestion, ont placé au centre de leurs préoccupations le rôle structurant des usages des technologies de l'information et de la communication (Orlikowski, 2000). Insistant tout particulièrement sur la nécessité de prêter attention à la dimension matérielle de ces technologies, ils se sont penchés sur leurs capacités à produire des cadres durables pour l'action collective et à solidifier des pratiques, des normes, voire des formes organisationnelles (Orlikowski, 2007 ; Leonardi, & Barley, 2008). Une telle perspective prend directement sa source chez Giddens et dans le courant de recherche qu'il est aujourd'hui convenu d'appeler le « structurationnisme ». Elle vise principalement à rendre compte de la dynamique de sédimentation progressive qui voit les usages de certaines technologies produire, à l'échelle même des pratiques ordinaires, des changements durables dans les organisations (Vaast, & Walsham, 2005). Elle doit aussi beaucoup à la sociologie des techniques, en particulier aux *Science and Technology Studies* (STS) dont on sait à quel point elles ont joué un rôle essentiel dans la réhabilitation des technologies et plus généralement des objets, dans l'analyse sociologique. Une grande majorité des travaux dans ces domaines ont en effet focalisé leurs analyses sur les processus de stabilisation des innovations techniques, faisant de la consolidation plus ou moins rapide des propriétés sociomatérielles d'une technologie un élément crucial de leurs modèles (Bijker, Hugues, & Pinch, 1989 ; Bijker et Law, 1992 ; McKenzie, & Wajcman, 1999).

C'est généralement par l'étude de phases en deux temps, faites d'un moment de crise (qui peut prendre la forme d'une controverse véhémente ou d'un accident) suivi d'un moment d'apaisement, que cette consolidation est étudiée. Le « succès » d'une innovation dépend ici de sa capacité à atteindre un degré de stabilisation telle que la technologie, quelle qu'elle soit, devienne un objet aux frontières hermétiquement close, un assemblage solide dont l'usage devient un allant-de-soi. On retrouve l'idée largement reprise en sciences de l'organisation qui veut que les technologies cristallisent peu à peu des aspects culturels, normatifs, économiques, sur le modèle désormais canonique de la bicyclette (Bijker, 1997).

Récemment, ces travaux ont fait l'objet de discussions approfondies et leur posture quasi unanime quant à la stabilisation et la clôture des innovations techniques a été remise en question. C'est sans doute Law qui a le mieux exposé les termes du débat en mettant en lumière les différences importantes qui se sont peu à peu installées entre chercheurs au sein des STS (Law, 2010). Sans entrer dans les détails, il faut surtout retenir qu'à une première posture qui insiste sur la « construction sociale » des technologies, Law oppose la démarche sémiotique (rassemblant les

---

[2] Cette recherche a été financée par le laboratoire SUSI de France Telecom R&D et réalisée avec l'aide de Damien Guillaume. Des entretiens approfondis ont été effectués auprès de prescripteurs de sécurité et d'usagers finaux dans 43 entreprises (une heure trente en moyenne), avec 17 responsables informatiques et 26 utilisateurs finaux. Dans le cadre de cet article, je m'appuierai essentiellement sur le discours des prescripteurs (responsables du système d'information, ou directement responsables de la sécurité informatique dans les entreprises les plus importantes), principaux représentants des politiques sécuritaires.

études féministes, post-coloniales et une partie de la théorie de l'acteur-réseau) qui vise principalement à élargir le vocabulaire de description des dynamiques d'innovation et des usages des technologies afin d'en saisir la variété[3]. Pour le dire simplement, il s'agit de ne pas nier les processus de solidification et de clôture, mais de ne plus en faire le seul et unique modèle (le seul « *mode of mattering* » possible, dans le vocabulaire de Law). Outre la rupture radicale, et désormais classique, qui consiste à ne pas décider à l'avance de ce qui relève du technique, du social, de l'économique, etc., et assumer pleinement le caractère relationnel des phénomènes observés, Law identifie deux éléments essentiels à considérer pour se détacher de la posture constructiviste : d'une part, l'hétérogénéité des assemblages technologiques (et l'incertitude forte qui caractérise les usages des outils les plus simples comme les plus complexes) ; et d'autre part la multiplicité des régimes de stabilisation sociotechnique (qui, s'ils peuvent s'aligner entre eux, peuvent aussi cohabiter, diverger, voire entrer en contradiction).

Les pistes ouvertes sont particulièrement stimulantes. D'abord parce qu'elles remettent en quelque sorte la sociologie des techniques à l'ouvrage en la confrontant à la complexité des phénomènes dont elle cherche à rendre compte et aux nombreux aspects que ses premiers travaux ont laissés inexplorés (Law, & Mol, 2001). Si les processus de rationalisation et d'ordonnancement ont très largement été étudiés, il reste en effet encore beaucoup à dire du *mess*, c'est-à-dire des situations d'inquiétude, de débordement, d'ignorance, de conflits non résolus, etc. (Law, 2004). Ces pistes sont riches également parce qu'elles poussent à adopter la posture scientifique défendue par Glaser et Strauss qui consiste à privilégier l'émergence théorique à partir d'enquêtes empiriques approfondies plutôt que la vérification toujours répétée de concepts passés (Glaser, & Strauss, 1967). Il y a un risque fort, en effet, à ce que les chercheurs se reposent sur leurs lauriers (et surtout ceux des autres) et que la sociologie des techniques véhicule des machines de guerre théoriques stériles. En introduction d'un ouvrage dédié précisément à l'évitement de ce risque, Law stigmatise par exemple l'usage « managérialiste » qui est fait depuis quelques années de certaines notions de la théorie de l'acteur-réseau (intéressement, boîte noire, mobile immuable) qui deviennent des mots porte-drapeau destinés à expliquer tout et son contraire (Law, 1999).

Objet de recherche hybride et protéiforme, les politiques ordinaires de sécurité informatique entrent parfaitement dans le cadre des préoccupations que revendique cette posture de recherche, aujourd'hui étiquetée sous l'acronyme « post-ANT »[4] (Gad, & Jensen, 2010). Elles installent au cœur des préoccupations de chacun un problème qui demeure un angle mort de la plupart des travaux de la sociologie des techniques : la fragilité matérielle. Elles offrent ainsi un site privilégié pour explorer un mode d'existence des nouvelles technologies mal connu, voire complètement ignoré.

Comment les politiques de sécurité informatique instaurent-elles la fragilité des technologies comme préoccupation partagée ? Quelle forme prend-elle ? Quelles pratiques sont-elles mises en œuvre en son nom ? Comment celles-ci travaillent-elles l'organisation et les places des uns et des autres au sein des entreprises ? La liste, à peine esquissée ici, des questions que soulève la sécurité informatique est immense. S'il n'est pas question évidemment de toutes les aborder ici, un premier moyen d'y répondre consiste à analyser en détail les principaux risques sur lesquels s'appuient les politiques de sécurité informatique pour définir leurs grands domaines d'action.

Risques informatiques et régime de fragilité permanente

Nous savons depuis Foucault (1994) que toute forme de gouvernementalité met indissociablement en œuvre savoir et pouvoir. Autrement dit, toute emprise sur le monde s'appuie sur une désignation propre des entités qui le composent et dont il s'agit de tenir compte. Les prescriptions sécuritaires dans le domaine informatique vont ainsi de pair avec des descriptions, plus ou moins précises, de propriétés sociales, techniques, matérielles, qui constituent le monde au sein duquel

---

[3] Ce faisant Law résume un travail réflexif initié en 1999 (Law, & Hassard, 1999) et repris de nombreuses fois par d'autres chercheurs , au premier rang desquels Mol (2002) et bien entendu Latour (2001, 2006).

[4] Pour post-Actor-Network Theory.

elles prennent formes. Autrement dit, elles produisent des ontologies (Mol, 1999 ; Boullier, Jollivet, & Audren, 2007). Parmi ce jeu de définitions et de désignations, celles qui sont relatives aux risques tiennent une place cruciale. Le travail des responsables de la sécurité informatique varie évidemment d'une entreprise à une autre et d'un secteur à l'autre, il reste toutefois toujours focalisé sur la production d'un souci sécuritaire partagé. Ce souci se fonde presque exclusivement sur la désignation de certains risques auxquels ils s'agit de sensibiliser différentes personnes au sein de l'entreprise (managers, utilisateurs finaux, ressources humaines…) ; risques qui dessinent les contours d'une fragilité technique spécifique.

Plutôt que s'en tenir aux documents officiels qui stabilisent un vocabulaire restreint dans le domaine, l'objectif de cette enquête était de comprendre comment les activités sécuritaires se déployaient quotidiennement dans les entreprises, afin notamment d'appréhender le périmètre effectif de ce dont les services dédiés à la sécurité avaient la charge. Durant les entretiens, trois types de risque ont ainsi été mis en avant : les premiers s'appuient sur la désignation d'un espace extérieur potentiellement dangereux, les seconds se présentent au contraire comme des risques internes liés à certaines pratiques qu'il faut chercher à encadrer, enfin, les troisièmes renvoient aux vulnérabilités matérielles des outils informatiques.

La figure de la contamination représente sans doute le plus connu des risques informatiques, le plus médiatisé. Au-delà de son apparente banalité, elle dessine un monde informatique très particulier. Elle place d'abord au centre de tous les regards le *virus*, entité directement venue de la biologie, au cœur de l'association étroite de l'informatique et du monde médical (Casilli, 2009). Mais le risque comme contamination donne aussi une certaine forme au réseau numérique lui-même : il en fait un *environnement* dans lequel les personnes comme les machines sont immergées. Cet environnement porte en lui d'autres dangers. Il est d'abord malsain, c'est-à-dire qu'y circulent un grand nombre d'éléments parasites et « sales » que l'on peut « attraper » par inadvertance. Mais il est aussi ouvert et public, deux qualités qui peuvent poser problème dans un cadre professionnel. Les échanges qui y ont cours sont susceptibles d'indiscrétions. À côté de la contamination, la figure de l'espionnage, voire du vol de données, tient donc une place importante. Enfin, le réseau en tant qu'environnement est peuplé d'êtres malintentionnés qui menacent d'attaques multiples les machines et les personnes qui s'y engagent.

Ce premier ensemble de risques fait notamment l'objet du travail des administrateurs de réseau qui se positionnent dans les organisations en « vigiles invisibles », prêts à sonner l'alerte lorsque les dangers approchent (Chateauraynaud, & Trabal 2007). Mais si les moments de crise comme l'attaque ou la contamination sont évidemment cruciaux, c'est surtout en tant que risques latents que les politiques sécuritaires traitent ces problèmes et prônent certaines solutions. Les dangers associés à la mise en évidence d'un réseau extérieur sont donc tout autant affaire de frontières que de vigilance. On trouve ici une première précision quant à la fragilité technique des systèmes informatiques : les protocoles d'échange et les machines elles-mêmes ont des frontières trop peu marquées et présentent des « failles » qui mettent à mal l'étanchéité que l'on cherche à construire pour la circulation des informations, les transactions, et souvent l'entreprise elle-même.

Dans ce cas de figure, l'idéal vers lequel tendent les politiques sécuritaires est proche des enseignements de la sociologie des techniques traditionnelle. Pour assurer la sécurité, il faut tenter de délimiter des points de passages contrôlés entre un intérieur et un extérieur définis dans un même mouvement. Il faut, plus généralement, assurer la stabilité des entités. Les mesures les plus courantes sont ainsi l'installation de *firewalls*, logiciels ou matériels, par lesquels sont censés passer tous les échanges, ou l'utilisation de réseaux privés cryptés (VPN) qui codent les échanges et qui sont présentés comme des « tunnels » informatiques.

> Donc, on monte un VPN, un Réseau Privé et Virtuel qui fonctionne comme un tunnel entre le matériel [de l'entreprise] et le réseau [de l'entreprise]. Et tout ce qui se passe là-dedans, tout ce qui passe dans ce réseau privé virtuel, est crypté, ça n'est pas attaquable par Internet… Et le vendeur travaille de chez lui comme s'il était physiquement dans un bureau de [l'entreprise] *(DSI, Industrie matière première)*.

Certaines opérations plus radicales donnent mieux encore à voir les enjeux de cette forme de risques. Pour le stock des données les plus sensibles, celles qui sont qualifiées de « stratégiques » (Denis, 2009a), certains services informatiques recommandent la déconnexion pure et simple, c'est-à-dire la mise en place d'un poste informatique dédié, qui n'est relié au réseau par aucune prise.

> Dans l'entreprise quand c'est secret, c'est uniquement étanche, hors flux, hors réseau. On travaille pour des clients qui sont la gendarmerie, qui sont l'État, des choses comme ça, là c'est stratégique. Et là, on a des salles [spécifiques], tout est dédié (*Ingénieur commercial, télé-communications*).

Ce jeu de frontières peut même aller au-delà d'Internet et concerner des formes d'intrusions physiques. La sécurité passe alors par la désactivation des ports USB, empêchant la lecture de cartes et de clés, ainsi que celle de supports externes accessibles par le lecteur de disques (CD-Rom, DVD).

La politique sécuritaire est ici affaire de territorialisation : celle du réseau qui participe à un extérieur menaçant (que ce soit à titre sanitaire ou militaire) et, dans le même mouvement, celle des machines et des communications qu'elles supportent, dont on s'attache à consolider les frontières. Une affaire de délimitation et de clôture, donc. Sauf qu'à la différence des cas habituellement étudiés par la sociologie des techniques, le temps de la clôture n'arrive jamais. Il n'y a pas d'apaisement complet dans le monde de la sécurité informatique. Les failles, parce qu'elles sont évidement en relation directe avec les progrès faits par les attaquants et leurs virus, sont une qualité (ou plutôt un défaut) permanente des technologies informatiques.

Ce point est plus saillant encore à propos d'un deuxième type de risques : celui qui porte sur les pratiques quotidiennes de l'informatique. Dans ce cas, il n'est pas question de pointer vers un extérieur duquel il faut se protéger, mais de souligner la vulnérabilité des données informatiques en tant que telles. C'est la permanence et la cohérence des systèmes d'informations que l'on cherche à protéger ici. La quantité des données et la complexité de leurs agencements apparaissent alors autant comme une force pour l'organisation qu'un danger. La facilité avec laquelle des informations peuvent être « déplacées » dans le système, ou remplacées par d'autres, est en point de mire de nombreux entretiens des prescripteurs de sécurité. Sous cet aspect, l'informatique est décrite comme un univers où les mauvaises manipulations sont nombreuses, d'autant plus qu'elles peuvent rester invisibles aux yeux des utilisateurs *lambda*.

Face à ce danger, les solutions consistent à rigidifier le système d'informations en empêchant certaines activités (la copie, le remplacement, le déplacement, le réécriture, le changement de nom…). Elles passent la plupart du temps par ce que nombre de responsables informatiques considèrent comme la clé de voûte de la sécurité : le *profiling*. Cette activité consiste à donner des droits d'accès, d'écriture, de lecture, de copie, etc. aux personnes en fonction de positions qui leur sont attribuées plus ou moins durablement. Sa mise en œuvre délicate montre à quel point le travail des services de sécurité informatique n'est jamais purement technique. Au découpage des fichiers, à l'élaboration d'arborescences consolidées répondent le découpage de l'organisation et la définition de l'identité des personnes et de leurs missions.

> On découpe les grands métiers de l'entreprise, ce qu'on autorise à faire ou pas par métier en fonction des niveaux hiérarchiques et des sectorisations géographiques? Ensuite, on met en place les outils ou les contrôles pour empêcher que… pour que la personne puisse faire vraiment ce qui est défini (*Responsable informatique, énergie*)

Je reviendrai sur les conséquences de ce type d'opérations. Ce qui importe ici, c'est l'instabilité que mettent en lumière les risques liés la désorganisation des données. Celle-ci n'est pas quelque chose que l'on peut régler une fois pour toutes. Elle est indissociable des pratiques mêmes de l'informatique en entreprise, pratiques qui visent justement à faciliter le travail collaboratif, l'organisation par projets et la souplesse d'accès à un nombre considérable de données. La multiplication des outils (postes fixes, portables, téléphones mobiles, agendas électroniques...), la porosité accentuée des frontières entre vie professionnelle et vie privée, l'accroissement des

circuits de communication, sont autant de facteurs de risque qui ne sont jamais envisagés comme des éléments contre lesquels lutter puisqu'ils sont précisément considérés comme des progrès de l'informatique professionnelle.

L'état de fragilité qui est mis en avant par certains responsables de sécurité informatique est ainsi un état permanent, une *donnée* du monde technique dans lequel ils évoluent. Un état qu'ils soulignent également lorsqu'ils évoquent le troisième type de risque en appréhendant les technologies sur leur plan matériel. Les machines sont fragiles : elles se cassent, se perdent, souffrent de la chaleur. C'est vrai des gros serveurs, qui font l'objet d'une attention particulière, et bénéficient de systèmes de climatisation, de protection électrique, etc. Mais de manière plus ordinaire, cette fragilité matérielle est au cœur du travail de sensibilisation que les prescripteurs font auprès d'usagers qu'ils jugent particulièrement « inconscients » de ce type de risques.

> Et puis après, il y a le côté aussi « sécurité » du matériel […], un portable qui tombe d'une table ou qui se cogne contre des portes ou des meubles, ça arrive aussi. […] Les plus tête en l'air peuvent l'oublier dans un train ou autre (*Responsable informatique, Services aux entreprises*).

Il faut donc que les utilisateurs se préoccupent des machines qu'on leur confie. Il leur est demandé de les traiter comme des entités délicates qui ne sont pas si solides qu'eux-mêmes pourraient le croire. Cette attention aux objets contraste fortement avec la notion même d'usages dont on perçoit ici les limites. Celle-ci présente généralement les nouvelles technologies comme des intermédiaires, ou au mieux des appuis, de l'action, qui peuvent faire l'objet d'une plus ou moins grande appropriation par ceux et celles qui les mobilisent. En contraste, la demande sécuritaire qui est faite aux usagers revient à centrer leur attention sur les technologies elles-mêmes (et non pas sur leurs fonctions, ni sur les activités qu'elles permettent de réaliser) : elle les invite à en prendre soin. Les politiques sécuritaires dessinent ainsi les contours d'un possible *care* des choses (Denis, & Pontille, 2011) sur lequel je reviendrai.

Plus généralement, les trois types de risque exposés ici dessinent un mode d'existence technique fondé sur une perpétuelle remise en cause de la solidité et de la fiabilité des outils informatiques. Cette remise en cause n'est pas extérieure : elle ne vient ni de la critique ni de la controverse. Elle est alimentée par les porte-parole des technologies eux-mêmes qui présentent la vulnérabilité comme une propriété des choses de l'informatique face à laquelle une attitude de vigilance permanente est nécessaire. De ce point de vue, la sécurité informatique ne cadre pas avec le modèle d'un régime d'apaisement des techniques qui associerait leur succès, ou leur « implémentation réussie », dans le vocabulaire du management, à leur consolidation progressive. Elle s'éloigne également des processus de cadrage des usages qui passent par la standardisation des technologies dans des propriétés intrinsèques stabilisées, ce que Thévenot appelle « l'immobilisation des choses » (Thévenot,1993).

Pour compléter cette première approche de la fragilité informatique appréhendée comme une propriété intrinsèque des technologies qui nécessite des formes d'attention spécifique, il faut passer de la description des risques aux prescriptions sécuritaires elles-mêmes.

Sécurité et impuretés sociotechniques

La production progressive de frontières nettes entre ce qui relève du technique et du social, la désignation de places claires pour les humains et les non-humains, sont des processus de « purification » (Latour, & Woolgar, 1988) essentiels aux modes d'existence des innovations techniques et scientifiques (Latour, 1991; Callon 1986) et à la stabilisation des technologies et de leurs usages. On trouve bien entendu des dynamiques de ce type dans les politiques ordinaires de sécurité informatique. En général, dans ce cas, la mise en œuvre de la sécurité est une affaire exclusivement réservée aux machines et aux paramétrages techniques. Mais, comme le laisse entendre l'importance des pratiques de sensibilisation évoquées plus haut, ces situations sont assez rares et ne sont pas celles qu'évoquent spontanément les responsables informatiques pour décrire leurs activités et plus généralement leurs politiques sécuritaires. Ce qu'ils mettent en avant illustre au contraire le caractère indissociablement sociotechnique de la sécurité informatique.

Cela est flagrant si l'on reprend le cas des pratiques de *profiling* évoquées plus haut. Définir les droits d'accès, de copie, ou d'écriture engage un délicat travail d'objectivation de structures organisationnelles que l'on tient généralement pour acquises mais qui se dérobent à la moindre tentative de description. Pour attribuer des profils, il faut, avant d'attribuer des droits, répondre à des questions abyssales telles que « qui fait quoi ? » ou « qui est à l'intérieur de l'entreprise, qui est à l'extérieur ? », voire « qui est qui ? ». Cette tâche immense est éminemment politique. Elle fait basculer le service informatique dans un véritable « travail organisationnel » (Strauss, 1988) qu'il ne peut mener seul. Elle montre à quel point informatique et organisation sont liées. À l'instar des démarches qualité, les politiques sécuritaires font *travailler* l'organisation (Cochoy, Garel, & de Terssac, 1999).

Cette articulation des problématiques techniques et organisationnelles déborde sur les rapports que les services informatiques entretiennent avec une partie de la hiérarchie. Certains responsables insistent ainsi sur la nature hybride des règles de sécurité qui sont élaborées dans le cadre de la gestion des droits et sur la nécessité d'un engagement fort de la ligne managériale. Ils expriment un net refus à endosser seuls des opérations qu'ils n'estiment pas de leur ressort, c'est-à-dire qu'ils ne considèrent pas comme purement techniques.

> Cette matrice de ségrégation de tâches, on va dire de « pouvoirs », l'informatique doit en être le garant. Mais la gestion de qui peut faire quoi, ce n'est pas l'informatique qui doit dire ça… Il faut que ça soit vraiment une application de la Direction Générale. […] Nous, nous sommes les garants, les gendarmes, mais nous ne sommes pas les prescripteurs (*Responsable informatique, énergie*).

Les relations entre les services informatiques et les autres parties de l'entreprise ne peuvent se réduire ni à la figure de la soumission à une règle aveugle, ni à celle de jeux de pouvoirs stratégiques où les uns chercheraient contre les autres à prendre la main sur tel ou tel aspect des questions sécuritaires pour assurer la réalisation de leurs objectifs. Ce que défendent les responsables de la sécurité, c'est une marche conjointe de plusieurs services qui fasse de la sécurité informatique un souci commun.

> Ce qu'il faut, c'est le relais des hiérarchies, c'est là que c'est important parce que, même quelque chose comme une note affichée qui dit « la sécurité, c'est vous », qui peut être très bien faite... Si la hiérarchie locale ne réexplique pas et ne remotive pas... n'intègre pas les opérationnels dans la démarche, ça ne marche pas bien. Et c'est un travail qui n'est pas fait partout, ça dépend des cultures de chefs (*Responsable informatique, énergie*).

La prescription de la sécurité ne semble pouvoir tenir que si elle est concrètement intégrée aux autres domaines réglementaires de l'organisation. Ce n'est qu'une fois prise dans cet ensemble d'actions d'encadrement qu'elle prend son sens véritable : une priorité « en tant que telle », qui ne se résume pas à quelques questions techniques clairement délimitées. Dans cette même veine, le travail de sensibilisation des utilisateurs est présenté comme étant idéalement le fruit d'une collaboration étroite entre services informatiques et services de communication. La mobilisation de tous autour des enjeux sécuritaires devrait être un objet de communication interne, bénéficiant de tous les moyens et les savoir-faire dont disposent les « communicants » de l'entreprise.

C'est une forme élargie de la solidarité sociotechnique qui est en jeu ici. Une solidarité qui repose sur le montage difficile d'« agencements organisationnels » (Girin, 1995) qui sont seuls capables, aux yeux des porte-parole de l'informatique, d'inscrire les principes sécuritaires dans le quotidien de l'entreprise.

Bien sûr, on sait cela depuis longtemps et il n'est pas question ici de mettre pour une énième fois en lumière le caractère hétérogène des technologies et de leurs usages. Ce qui importe dans le cas précis de la sécurité informatique, c'est le rôle que tient cette hétérogénéité sociotechnique dans les prescriptions elles-mêmes. Plutôt que de défendre coûte que coûte un pré carré (qui, selon les termes classiques de la sociologie des organisations, leur donnerait une forme de pouvoir), ou d'assurer au quotidien la « pureté » technique des outils en invisibilisant toute action humaine, les prescripteurs techniques revendiquent eux-mêmes une certaine hybridité et refusent

de faire de la sécurité informatique la préoccupation des seules machines et de leurs techniciens. Cette posture se retrouve dans la manière dont certains responsables de la sécurité cherchent à mobiliser les utilisateurs finaux.

Il existe bien entendu de nombreux dispositifs sécuritaires qui incorporent durablement dans la technologie des actions essentielles sous formes de scripts automatisés et de tâches de fond sur lesquelles les usagers n'ont pas la main. On a alors affaire à des formes de prescription forte qui délèguent une part du suivi de la règle à l'environnement et reposent sur un confinement technique de l'action (Hatchuel,1996 ; Denis, 2007). Dans ce cas, les rapports entre usagers et services informatiques peuvent être conflictuels, les seconds étant accusés d'entraver les activités professionnelles des premiers, tandis qu'inversement ceux-ci reprochent aux usagers de compliquer leur travail par leurs ajustements et autres tentatives de détournement des procédures techniques. Posé ainsi, le geste principal de la prescription de la sécurité informatique consiste à opérer des choix pour équilibrer exigences sécuritaires et exigences professionnelles. Cela est par exemple très clairement affirmé dans un article « témoignage » du numéro 49 de la *Lettre Sécurité Informatique du CNRS* (juin 2004). Un administrateur système d'un laboratoire de Chimie théorique s'y exprime sous le titre « Sécurité informatique et besoins des utilisateurs : un compromis difficile ».

Mais il ne faut pas s'arrêter à cette première image des rapports entre services techniques et utilisateurs. Pour certains prescripteurs cette forme de solidarité sociotechnique fondée sur la soumission et le partage clair entre technique et humains n'est pas satisfaisante. Ils défendent au contraire l'idée d'un monde aux préoccupations partagées, dans lequel la sécurité informatique forme une chaîne explicitement hétérogène. Dans ce monde, la sécurité technique « totale », c'est-à-dire entièrement réalisée dans des scripts, est impossible, en tout cas impensable. Nous l'avons vu à propos des agencements organisationnels qui se constituaient avec la ligne hiérarchique, mais cela est plus frappant encore à propos du rôle des usagers.

> On sait aussi que la sécurité, ça repose surtout sur les hommes. C'est-à-dire sur le fait que les utilisateurs de l'informatique acceptent les règles de la sécurité et les acceptent et puis font normalement attention à la protection de ce qu'ils transportent : pas se faire voler son PC, pas se faire voler son téléphone (*Administrateur réseau, transports*).

L'implication de tout le monde dans le processus est considéré comme la pierre de touche de la sécurité informatique. Cela se traduit par un grand nombre de stratégies d'enrôlement qui vont au-delà des enjeux de sensibilisation et de communication. L'objectif ici est de faire agir les usagers au sens fort du terme, et de les engager dans des opérations dont ils ont véritablement « conscience », et dont ils sont responsables au sens large du terme. Dans sa version la plus radicale, cette politique passe par le refus d'implanter certains automatismes techniques pourtant répandus.

> On a des serveurs de sauvegarde, si les gens veulent. Mais les gens sont libres, les gens sont libres de placer leurs documents là où ils veulent s'ils veulent les sauvegarder. Parce qu'ils peuvent les mettre sur leurs machines, ils peuvent aussi les laisser sur les serveurs. […] Mais ils font ce qu'ils veulent. S'ils veulent sauvegarder, ils sauvegardent, s'ils ne veulent pas, ils… Enfin, ce que je veux dire… après, c'est à leur risque et péril (*Responsable informatique, services aux entreprises*).

Dans cette logique, on voit clairement les liens qui existent entre le point soulevé plus haut (la prise de conscience de la vulnérabilité de l'informatique) et l'hybridation sociotechnique des politiques sécuritaires. Si les machines se mettent à sauvegarder les données d'elles-mêmes, de manière fluide et sans aucune visibilité, les personnes risquent de perdre de vue l'importance de ces opérations de sauvegarde et, au-delà, d'oublier la fragilité intrinsèque des données informatiques.

> Charge à l'utilisateur de régulièrement, de lancer son back-up. Régulièrement, une fois par semaine, donc ça peut représenter cinq, dix mégas par semaine à envoyer… Maintenant, si vous attendez la fin de l'année bon, ça fait beaucoup plus. Le différentiel est important. Donc, vous avez un… un volume

> important à pousser. [C'est à l'utilisateur de faire une manipulation particulière ?].C'est à l'utilisateur de faire la manipulation parce que chez nous, l'utilisateur est responsable de ses données. S'il les perd, s'il perd ses prospects, les documents qu'il échange avec ses clients, s'il perd ses feuilles Excel, il perd tout ça, c'est son problème. (*DSI, Industrie matière première*).

C'est donc un enjeu de visibilité et d'invisibilité qui est soulevé, comme dans le cas des administrateurs de réseau qu'étudient Chateauraynaud et Trabal (2007). Mais c'est moins la visibilité des personnels techniques dédiés à la sécurité qui est en jeu ici que celle des opérations elles-mêmes et, en miroir, celle de la vulnérabilité des dispositifs techniques.

Sur ce plan, la plupart des politiques sécuritaires se traduisent par des opérations de communication qui visent à sensibiliser les personnes. Mais pour certains prescripteurs, il faudrait aller plus loin et placer la part humaine du dispositif sécuritaire au centre des exigences professionnelles. Pour eux, avoir conscience des problématiques de sécurité, savoir comprendre les risques encourus ne sont pas tant des éléments auxquels sensibiliser que des compétences essentielles au travail, des critères relevant de la gestion même des ressources humaines. Le cas des activités militaires, figure paradigmatique du secteur sécuritaire, offre une illustration idéale de cette manière de voir les choses.

> Et même... [la sécurité] la plus complète possible n'est pas complète et de toute façon. Même le secret défense ou les choses qui doivent être gardées... […] Outre le fait que c'est économiquement irréaliste, je pense que c'est même pratiquement infaisable. Même les militaires, ils ont des personnels assermentés. Éventuellement, ils font des enquêtes sur la capacité de ces personnes, la capacité supposée de ces personnes à se conduire comme il convient en face des secrets qu'ils détiennent (*Administrateur réseau, transports*).

Autrement dit, il est demandé aux usagers de ne pas prendre les technologies informatiques pour des « boîtes noires », au sens de la théorie de l'acteur-réseau, sur lesquelles ils pourraient s'appuyer aveuglément. Pour certains responsables de la sécurité, les usagers doivent être capables, pour assurer le fonctionnement quotidien des systèmes d'informations et des outils qui les alimentent, de participer à la marche commune de la sécurité et, plus encore, de prendre conscience de sa difficulté et de ses coûts. Et c'est sur ce point précis, cette exigence de conscience et de responsabilité, que les tensions entre usagers et services techniques se cristallisent. Car certains usagers sont quant à eux demandeurs de boîtes noires, c'est-à-dire d'une gestion purement technique de la sécurité.

> C'est sûr, il y a des sécurités à tire-larigot. Mais nous, on n'est pas au courant… chacun son métier. C'est-à-dire nous, nous sommes des commerciaux, on nous communique des outils pour communiquer, pour améliorer notre quotidien, mais les problèmes d'informatique, bon, ça passe au-dessus de moi. Je veux dire : ça n'est pas mon problème. Moi, je suis un commercial, je suis rémunéré pour… Je ne suis pas payé pour voir les problèmes d'informatique (*Commercial, santé*).

Ou encore :

> Non, je ne m'occupe de rien. […] Chacun fait son boulot. L'informatique, leur job à eux, c'est de sauvegarder, crypter, vérifier que tout fonctionne bien et moi, je fais mon job. Moi, ça se résume à appuyer sur une touche pour crypter mes données, point (*Ingénieur R&D, Aéronautique*).

L'image d'un monde hybride dans lequel la sécurité serait une préoccupation qui reposerait tant sur les hommes que sur les machines n'est donc pas partagée. Lorsqu'elles prennent une forme exclusivement technique, les règles de sécurité passent par des scripts qui ne posent des problèmes qu'à la marge. Mais les choses se compliquent dès lors qu'il s'agit d'assembler personnes et machines dans des composites sociotechniques qui sont considérés par les responsables de l'informatique comme les seuls garants d'une sécurité efficiente. La mise en place des solidarités sociotechniques prend alors une dimension politique et se joue dans la négociation délicate et jamais stabilisée des positions de chacun (Denis, 2009b).

Ce travail d'agencement est très éloigné des procédés de purification que l'on a l'habitude d'observer dans le cadre de la sociologie et de l'histoire des techniques. Celles-ci nous donnent en effet généralement à voir des cas où la stabilité (toujours provisoire) des dispositifs techniques, et leur intégration dans la vie quotidienne, passent par des jeux de séparation nette entre le social et la technique. Si l'on retrouve bien cette dynamique du côté des utilisateurs réticents à prendre en charge des opérations ou des attitudes qu'ils souhaiteraient cantonnées au monde technique, la posture des porte-parole des technologies informatiques s'y oppose complètement lorsqu'ils revendiquent l'impureté de l'informatique et en font une condition explicite de sa sécurité quotidienne.

Les grandes lignes des résultats présentés ici montrent comment les politiques de sécurité informatique sont tournées vers l'installation d'un souci partagé pour la vulnérabilité technique, non pas comme le moteur d'une remise en cause des technologies, mais comme manière convenable de traiter avec les choses de l'informatique. C'est au nom de l'informatique et de son bon fonctionnement que la fragilité est pointée comme un objet de préoccupations nécessaires. Pour tenter de comprendre les implications théoriques auxquelles mène cette piste, il faut se détacher du seul domaine de la sécurité informatique. Il n'est pas question en effet de suggérer que l'informatique serait un cas particulier, un objet qui n'entrerait pas complètement dans les cases des analyses en termes de construction sociale des technologies ou de théorie de l'acteur-réseau. Elle apporte en revanche un éclairage particulier mais central sur la spécificité des actions dédiées à fragilité technique.

Ni routine, ni crise : fragilité et travail de maintenance

Partir de situations où la fragilité technique est une préoccupation centrale est un premier mouvement dans la remise en cause d'un modèle qui se focaliserait exclusivement sur les processus de stabilisation et de clôture technologiques. Le cas de la sécurité informatique et du régime de fragilité permanente que ses porte parole défendent offrent de ce point de vue un large champ pour l'analyse. C'est tout particulièrement le refus, défendu par les prescripteurs techniques eux-mêmes, d'instaurer un certain nombre d'outils informatiques en boîtes noires qui invite à prolonger la discussion avec la sociologie des techniques, en particulier avec le courant constructiviste. Mais c'est moins sur les notions de stabilisation et de construction sociale que celle-ci doit porter, que sur la posture temporelle adoptée pour étudier les technologies et leurs usages.

L'analyse constructiviste illustre généralement les processus d'hybridation sociotechnique en insistant sur des moments particuliers de l'histoire des technologies qui s'achèvent par la cristallisation au sein d'un dispositif sociotechnique d'enjeux sociaux, politiques, culturels, économique, etc. Cette dynamique repose toujours sur deux temps bien distincts : celui de la crise (qu'elle prenne la forme d'une controverse technique, d'une affaire publique ou d'un accident), durant laquelle les propriétés sociotechniques sont mouvantes, en suspens ; suivi d'un apaisement, une fois la clôture réussie, c'est-à-dire l'installation durable d'une version solide du dispositif dont les frontières et les usages, s'ils ne sont évidemment pas univoques, redeviennent stables. Ces moments d'apaisement ne sont jamais présentés comme irrévocables : ils peuvent à tout moment faire l'objet d'une nouvelle crise. C'est sur ce rythme que l'incertitude est intégrée au modèle de la construction sociale des technologies. On retrouve dans ce mouvement, à une échelle collective, la différence que fait Heidegger entre des situations où un outil est *ready-to-hand*, manipulé par leurs usagers de manière transparente et celles, pannes ou casse, qui le rendent *present-at-hand*, objet d'attentions et de doutes (Verbeek, 2006).

Ce cadre explicatif fonctionne en partie pour les politiques sécuritaires. Il y a de grandes crises, des pannes, des attaques mémorables, qui remettent en cause les solutions déployées jusqu'ici et ouvrent les débats à de nombreux acteurs hétérogènes ; des contaminations qui déstabilisent des systèmes entiers qu'il faut ensuite remettre en ordre. Mais, nous l'avons vu, il ne permet pas de comprendre le quotidien des pratiques sécuritaires. La position de la plupart des responsables de

sécurité informatique interrogés consiste précisément à ne pas se focaliser sur les seuls moments exceptionnels. La vulnérabilité technique sur laquelle ils insistent est un état permanent. L'informatique qu'ils pratiquent et qu'ils cherchent à faire exister au sein des entreprises n'est jamais au repos, elle est faite de technologies qu'il ne faut pas considérer comme stabilisées, dont il ne faut jamais faire des allant de soi. En d'autres termes, les prescripteurs de sécurité semblent s'évertuer à ce que personne ne manipulent les outils informatiques de manière transparente, *ready-to-hand*, mais en y prêtant toujours une certaine attention.

Une telle manière d'envisager les objets techniques, et le rapport que l'on entretient avec eux, n'a rien de spécifique à l'informatique. Elle est en fait partagée par un grand nombre d'acteurs, généralement invisibles, dont le métier consiste précisément à prendre soin des choses. Qu'ils évoluent dans le domaine du nettoyage, de l'entretien ou de la réparation, ces personnes se chargent du *travail de maintenance* dont l'une des spécificités est précisément la permanence et le perpétuel recommencement (Denis, & Pontille, 2010a). La saleté, les dégradations, l'usure, etc. ne composent pas des évènements dans le cycle de vies des objets techniques. Ils adviennent quotidiennement et progressivement. Le travail de maintenance ne relève ainsi ni de la panne, ni de l'usage apaisé : il repose sur une vigilance constante qui forme un *continuum* entre routine et crise (Chateauraynaud, & Torny 1999). Cette vigilance n'est toutefois pas tout à fait celle des lanceurs d'alertes qui guettent les risques de loin (Chateauraynaud & Trabal 2007). Elle est beaucoup plus ordinaire et implique un rapport de proximité très grande avec les choses sur lesquelles elle porte. Le travail de maintenance s'appuie sur un type d'engagement avec les choses que l'on pourrait qualifier, s'inspirant de Thévenot (2006), de familiarité inquiète. Il est proche des formes de soin et d'attention à l'autre que Mol a décrites dans son ouvrage dédiée aux pratiques du *care* (Mol, 2008), notamment parce qu'il nécessite des compétences très spécifiques, littéralement hors normes, et qu'il prend comme point de départ, comme « norme », le caractère fragile et dégradable des choses (Denis, & Pontille, 2011).

S'intéresser à la fragilité des outils informatiques invite ainsi à se dégager d'une sociologie des techniques largement focalisée sur les dynamiques historiques d'innovation pour développer un modèle qui puisse prendre en considération le monde avec lequel traite les travailleurs de la maintenance. Quelques chercheurs ont déjà montré l'importance qu'il y avait à se préoccuper de cette face des technologies qui reste largement méconnue (Orr, 1999 ; Henke, 2000 ; Graham et Thrift, 2007). Le mouvement théorique qu'ils défendent consiste à partir des analyses de H. Garfinkel (1967) et de E. Goffman (1991) sur la vulnérabilité de l'ordre social et les pratiques incessantes de réparation qu'il nécessite, afin d'y intégrer les objets techniques. Tout comme l'ordre social, l'ordre matériel n'est jamais installé une fois pour toutes (pas même à « moyen terme »). Il est le produit d'un travail constant fait de surveillance et de petites réparations, souvent invisibles. L'ordre des choses, la stabilité des technologies, sont maintenus au jour le jour par des personnes qui traitent les objets au nom de leurs vulnérabilités et prennent soin d'eux.

C'est dans ce rythme particulier que s'engagent les prescripteurs techniques, faisant de la vulnérabilité des outils informatiques une préoccupation quotidienne, qu'ils cherchent à faire adopter au collectif hybride qui composent les chaînes sécuritaires. La sécurité informatique donne toutefois à voir un travail de maintenance bien particulier. Généralement, les opérations de maintenance relèvent d'un travail d'infrastructure (Star, & Ruhleder 1996) : elles sont menées de manière complètement invisible pour les utilisateurs. Dans un cas comme la signalétique du métro, nous avons par exemple montré que le travail de maintenance consistait à produire quotidiennement une solidité et une stabilité dirigées vers les usagers du métro par le biais d'activités menées en coulisses et prises en charge par des experts spécialisés (Denis, & Pontille, 2010b, chap. 5). Ces activités reposent sur des formes d'engagement avec les objets qui permettent de repérer les instabilités avant qu'elles n'éclatent au grand jour. En ce sens, la maintenance est relativement différente des activités de réparation à proprement parler (Denis, & Pontille, 2010a).

Or, nous l'avons vu, dans le cas de la sécurité informatique, il n'est pas question de scinder le monde entre activités de maintenance invisibles et usagers disposant d'outils sur lesquels ils peuvent s'appuyer de manière transparente. Cette question est précisément au cœur des tensions entre certains utilisateurs qui souhaitent s'appuyer sur des dispositifs sécuritaires invisibles et des

responsables de la sécurité qui cherchent à enrôler les usagers dans la danse de la maintenance. Il n'est pas question pour les prescripteurs de maintenir le monde en état à l'insu de ses habitants, en développant des savoir-faire spécifiques et en défendant un pré-carré d'activités hermétique. Au contraire, la maintenance semble n'être possible aux yeux de certains qu'à condition de devenir une pratique partagée au sein de laquelle la fragilité des objets techniques devient un souci commun.

C'est à un véritable *care* des choses qu'invitent ces prescripteurs techniques, sur le modèle des pratiques que l'on peut observer dans le domaine de la santé, pratiques partagées par le personnel soignant au sens large, mais aussi par les proches du patients eux-mêmes et un grand nombre d'acteurs qui ne sont pas experts médicaux (Mol, 2008). C'est sans doute la principale particularité de la maintenance mise en œuvre dans le cadre de la sécurité informatique : elle fait de la fragilité technique non pas seulement une affaire de spécialistes, mais une propriété intrinsèque, une ontologie, dont tout le monde doit avoir conscience.

Conclusions

L'ouvrage *Actor Netwok Theory and after?* dirigé par Law et Hassard (1999) a posé la première pierre d'une série de travaux qui sont aujourd'hui rangés sous l'étiquette « post-ANT » (Gad, & Jensen 2010). La recherche menée par De Laet et Mol (2000) reprise ensuite par Law est sans doute la plus emblématique de ce mouvement qui cherche à se détacher de l'enfermement progressif de la sociologie des techniques. Elle porte notamment sur la question des « mobiles immuables » chère à Latour (1985) et le mésusage qui en a été fait dans d'innombrables reprises. En prenant le cas de la pompe du désert au Zimbabwe, De Laët et Mol montrent qu'une technologie peut avoir du succès sans passer par un processus de stabilisation : la pompe est sans arrêt modifiée aménagée, et son inventeur lui-même défend une position d'ouverture complète, refusant de clore la technologie. De Laet et Mol en concluent que cette pompe est un « objet fluide », un « mobile muable » qui ne peut pas être décrit dans le modèle traditionnel de l'anthropologie des techniques.

Dans les travaux suivants, Mol et Law reprennent régulièrement cet exemple pour en souligner les conséquences théoriques : si les objets fluides passent en quelque sorte à travers les mailles de la sociologie des techniques, et d'une version dure de la théorie de l'acteur-réseau, c'est que ces modèles véhiculent des ontologies implicites qu'il faut savoir dépasser (Law, & Mol, 2001). Il faut inventer la voie pour une véritable politique des ontologies (Mol, 1999) et renforcer encore l'exigence d'ouverture analytique et de symétrie. C'est dans ce programme que s'inscrit l'enquête exposée ici, qui souligne, en contraste du vocabulaire de la solidité et de l'immuabilité, l'importance de la fragilité comme mode d'existence de la technique.

La posture analytique de Mol et Law permet de développer une attention affûtée à la dimension éminemment relationnelle des formes d'organisations sociotechniques. Refusant de réduire la variabilité des réalités observées à des jeux de perspectives interprétatives, elle laisse la voie ouverte à la multiplicité des objets, soulignant dans le même temps le caractère performatif de tout compte rendu, y compris sociologique, sur le monde (Law, & Singleton, 2005). Elle invite à comprendre que les phénomènes que l'on observe sont multiples, non pas parce qu'ils sont le résultats de perspectives interprétatives différentes[5], mais parce qu'ils sont actualisés par des dispositifs de description et de gouvernement spécifiques qui font émerger des ontologies variables. Une telle posture permet d'accepter pleinement le caractère paradoxal du succès des outils informatiques dans les entreprises : les technologies sont *à la fois* (par moments et pour certaines personnes) des boîtes noires, des objets techniques aux frontières à peu près clairement définies et stables, et des assemblages fragiles, vulnérables à un grand nombre de risques. L'un n'empêche pas l'autre, et le chercheur ne doit pas chercher à réduire à tout prix son analyse à un unique aspect.

---

[5] Ce que Latour a lui même intégré à son programme aujourd'hui : « Et cela n'a rien avoir avec la "flexibilité interprétative" qui permettrait de posséder sur une "même" chose de "multiples points de vue" : *c'est la chose elle-même à qui on laisse déployer sa multiplicité* […] » (Latour, 2006, p. 168).

Cette manière d'explorer continuellement des formes sociotechniques qui mettent à l'épreuve, pour les compléter sans forcément les discréditer, les modèles d'explication dominants de la sociologie des techniques, a évidemment des implications méthodologiques. Elle s'appuie notamment sur deux choix : celui des objets de recherche et celui des points d'entrée empiriques par lesquelles les chercheurs les appréhendent. Ces choix jouent un rôle essentiel dans le décalage théorique qu'il s'agit d'effectuer.

Ainsi, pour avoir accès à la fragilité technique, il a fallu faire ici un double mouvement. Observer d'abord des technologies qui n'étaient pas en situation de crise ou de controverse, mais prises dans le quotidien de leurs usage et de leur entretien. Ce geste méthodologique est en rupture avec la sociologie des techniques constructiviste et une partie des premiers travaux de la théorie de l'acteur-réseau qui se sont fondés sur l'étude des pannes et des controverses (Callon, 2006). Cette focalisation tient notamment à l'hypothèse d'un monde d'après les controverses, apaisé et routinier dans lequel les agencements sociotechniques et les vulnérabilités sont consolidés et largement invisibles. Celle-ci est évidemment largement confirmée, mais elle laisse de côté des formes d'instabilité qui ne relèvent ni de la critique ni de la panne radicale.

Le second mouvement porte sur les lieux de l'enquête. Plutôt que les innovateurs ou les utilisateurs, c'est un troisième type de personnes qui ont eu la parole ici : celles qui ont la charge de services que l'on appelle « support » dans les entreprises, et qui réparent et entretiennent quotidiennement les technologies. Ce sont elles qui se préoccupent de fragilité et qui vivent dans un monde jamais complètement apaisé. En allant à leur rencontre, nous avons pu voir que la stabilité et la clôture de technologies aussi répandues que l'informatique de bureau étaient toutes relatives, et plus encore, qu'elles n'étaient pas une fin en soi.

Références

Akrich, M., Callon, M. & Latour, B. (Eds.). (2006), *Sociologie de la traduction : Textes fondateurs*, Paris, Presses des Mines ParisTech.

Bijker, W. E. (1997), *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*, Cambridge: The MIT Press.

Bijker, W. E. & Law, J. (Eds.). (1994), *Shaping Technology / Building Society: Studies in Sociotechnical Change*, Cambridge: The MIT Press.

Bijker, W. E., Hugues, T. P. & Pinch, T. (Eds.). (1989), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, Cambridge: The MIT Press.

Boullier, D., Jollivet, P. & Audren, F. (2007), « Security : always too much and never enough », Anthropology of a non-starter market. *Annales des Télécommunications*, 62(11-12), 1274-1292.

Callon, M. (1986), « Éléments pour une sociologie de la traduction. La domestication des coquilles Saint Jacques et des marins pêcheurs dans la baie de Saint Brieuc », *L'Année sociologique*, (36), 169-208.

Callon, M. (2006), « Pour une sociologie des controverses technologiques », In M. Akrich, M. Callon, & B. Latour (Eds.), *Sociologie de la traduction. Textes fondateurs* (pp. 135-157). Paris, Presses des Mines.

Casilli, A. (2009), « Le stéthoscope et la souris : savoirs médicaux et imaginaires numériques du corps », *Esprit*, (353), 175-188.

Chateauraynaud, F. & Torny, D. (1999), *Les sombres précurseurs, une sociologie pragmatique de l'alerte et du risque*, Paris, Éditions de l'EHESS.

Chateauraynaud, F. & Trabal, F. (2007), « Des vigiles invisibles. Les administrateurs-réseaux et la sécurité informatique », *Annales des Télécommunications*, 62(11-12).

Cochoy, F., Garel, J.-P. & de Terssac, G. (1998), « Comment l'écrit travaille l'organisation : le cas des normes ISO 9000 », *Revue française de sociologie*, XXXIX(4), 673-699.

Denis, J. (2007), « La prescription ordinaire. Circulation et énonciation des règles au travail », *Sociologie du Travail*, 49(4), 496-513.

Denis, J. (2009a), « Sécurité informatique et valeur des écrits au travail », *Semen*, (28), 85-100.

Denis, J. (2009b), « Les ressorts de la sécurité informatique. Des hommes, des machines et des données », In C. Licoppe (Ed.), *L'évolution des cultures numériques, de la mutation du lien social à l'organisation du travail* (pp. 190-199). Paris, FYP.

Denis, J. & Pontille, D. (2010a), « Performativité de l'écrit et travail de maintenance », *Réseaux*, (163), 105-130.

Denis, J. & Pontille, D. (2010b), *Petite sociologie de la signalétique. Les coulisses des panneaux du métro*, Paris, Presses Mines ParisTech.

Denis, J. & Pontille, D. (2011), « Materiality, Maintenance and Fragility. The Care of Things », *"How Matter Matters", Third International Symposium on Process Organization Studies* (http://ssrn.com/abstract=1947255).

Foucault, M. (1994), *Dits et Ecrits, 1954-1988. Tome III : 1976-1979,* Paris, Gallimard.

Gad, C. & Jensen, C. B. (2009), « On the Consequences of Post-ANT », *Science, Technology & Human Values*, 35(1), 55-80.

Garfinkel, H. (1967), *Studies in ethnomethodology*, Englewood-cliffs, Prentice-Hall

Girin, J. (1995), Les agencements organisationnels », In F. Charue-Duboc (Ed.), *Des savoirs en action* (pp. 233-279). Paris, L'Harmattan.

Glaser, B. & Strauss, A. (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Chicago, Aldine Transaction.

Goffman, E. (1991), *Les cadres de l'expérience*, Paris, Minuit.

Graham, S. & Thrift, N. (2007), « Out of Order: Understanding Repair and Maintenance », *Theory, Culture & Society*, 24(3), 1-25.

Hatchuel, A. (1996), « Coopération et conception collective. Variétés et crises des rapports de prescription », In E. Friedberg (Ed.), *Coopération et conception* (pp. 101-121). Toulouse: Octares.

Henke, C. R. (2000), « The Mechanics of Workplace Order: Toward a Sociologgy of Repair », *Berkeley Journal of Sociology*, 44, 55-81.

De Laet, M. & Mol, A. (2000), « The Zimbabwe Bush Pump: Mechanics of a Fluid Technology », *Social Studies of Science*, (30), 175-180.

Latour, B. (1985), « Les "Vues " de l'esprit. Une introduction à l'anthropologie des sciences et des techniques », *Culture Technique*, 14, 4-29.

Latour, B. (1991), *Nous n'avons jamais été modernes. Essai d'anthropologie symétrique*, Paris, La découverte.

Latour, B. (2001), *L'espoir de Pandore. Pour une version réaliste de l'activité scientifique*, Paris, La Découverte.

Latour, B. (2006), *Changer de société, refaire de la sociologie*, Paris, La Découverte.

Latour, B. & Woolgar, S. (1988), *La vie de laboratoire*, Paris, La Découverte.

Law, J. (2004), *After Method: Mess in Social Science Research*, New York, Routledge.

Law, J. (2010), « The Materials of STS », In D. Hicks & M. C. Beaudry (Eds.), *The Oxford Handbook of Material Culture Studies* (pp. 173-188). Oxford, Oxford University Press.

Law, J. & Hassard, J. (1999), *Actor Network Theory and After*, Oxford, Wiley-Blackwell.

Law, J. & Mol, A. (2001), « Situating Technoscience: An Inquiry into Spatialities », *Society and Space*, 19, 609-621.

Law, J. & Singleton, V. (2005), « Object Lessons », *Organization*, 12(3), 331-355.

Leonardi, P. & Barley, S. (2008), « Materiality and change: Challenges to building better theory about technology and organizing », *Information and Organization*, 18(3), 159-176.

MacKenzie, D. & Wajcman, J. (Eds.). (1999), *The Social Shaping of Technology*, Manchester, Open University Press.

Mol, A. (1999), « Ontological politics. A word and some questions », In J. Law & J. Hassard (Eds.), *Actor Network Theory and After* (pp. 74-89). Oxford, Wiley-Blackwell.

Mol, A. (2002), *The Body Multiple: Ontology in Medical Practice*, London, Duke University Press Books.

Mol, A. (2008), *The Logic of Care: Health and the Problem of Patient Choice*, New York, Routledge.

Orlikowski, W. J. (2007), « Sociomaterial Practices: Exploring Technology at Work », *Organization Studies*, 28(9), 1435-1448.

Orlikowski, Wanda J. (2000), « Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations », *Organization Science*, 11(4), 404-428.

Orr, J. E. (1996), *Talking About Machines: An Ethnography of a Modern Job*, New York, Cornell University Press.

Star, S. L. & Ruhleder, K. (1996), « Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces », *Information Systems Research*, 7(1), 111-134.

Strauss, A. (1988), « The articulation of project work: an organizational process », *Sociological Quarterly*, 29(2), 163-178.

Thévenot, L. (1993), « Essai sur les objets usuels. Propriétés, fonctions, usages », In B. Conein, N. Dodier, & L. Thévenot (Eds.), *Les objets dans l'action. De la maison au laboratoire* (pp. 85-111). Paris, Éditions de l'EHESS.

Thévenot, L. (2006), *L'action au pluriel. Sociologie des régimes d'engagement*, Paris,New York, La Découverte.

Vaast, E. & Walsham, G. (2005), « Representations and actions: the transformation of work practices with IT use », *Information and Organization*, 15(1), 65-89.