Les ressorts de la sécurité informatique

Jérôme Denis

Les ressorts de la sécurité informatique
Des hommes, des machines et des données

Jérôme DENIS
LTCI (UMR5141) CNRS - TELECOM ParisTech
Département Sciences Économiques et Sociales
jerome.denis@telecom-paristech.fr

(2009) in C Licoppe (ed.), *L'évolution des cultures numériques, de la mutation du lien social à l'organisation du travail*, FYP, Paris (p. 190-199).

En parallèle de l'essor du marché des nouvelles technologies, on voit apparaître depuis quelques années une insistance de plus en plus grande sur les questions relatives à la sécurité informatique. De nombreux acteurs, y compris au sein des médias généralistes, mettent en avant ce qui semble être le prix à payer de l'entrée dans la société de l'information : les risques liés aux technologies numériques sont de plus en plus grands, et il est urgent de transformer nos comportements et d'adopter les équipements et les services qui permettent de s'en prémunir efficacement.

Les conditions du développement considérable des technologies électroniques de communication dans les entreprises sont donc contradictoires. 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 de ces dispositifs semble fragiliser. Virus, intrusions, pannes, sont les dangers ordinaires d'une société de l'information où la communication, la circulation des informations, la constitution et le partage de connaissances apparaissent dans le même temps facilités et menacés.

On connaît assez bien ce type de discours d'alerte qui fait partie d'un ensemble plus vaste tourné vers la sensibilisation du grand public aux problématiques sécuritaires[1]. Mais on sait moins comment cette préoccupation se déploie concrètement au sein des entreprises. C'est pourtant à cette échelle que réussissent ou échouent les politiques sécuritaires. Et c'est en étudiant leurs conditions et leurs conséquences quotidiennes que l'on peut comprendre ce que "sécuriser" veut dire. Quels sont les ressorts de la sécurité informatique en entreprise ? Quelles formes prennent les arguments liés à la sécurité informatique ? Comment se diffusent-ils ? À quelles activités donnent-ils lieu ?

L'objet est vaste et il n'est pas question de prétendre ici en embrasser la complexité[2]. Toute politique sécuritaire s'appuie par exemple sur une désignation de dangers qui sont non

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

[2] Ce chapitre s'appuie sur une recherche financée par le laboratoire SUSI de France Telecom R&D. Celle-ci a été suivie par Emmanuel Kessous et réalisée avec l'aide de Damien Guillaume. Des

seulement identifiés, qualifiés, mais aussi mis en scène de manières spécifiques. Plus généralement, les discours liés à la sécurité informatique composent un monde à part, fait d'entités qu'il faut savoir mobiliser, considérer attentivement, voire traiter avec précaution. Parmi l'ensemble de ce qui fait une politique sécuritaire, deux points retiendront notre attention ici. Le premier concerne l'"objet" de la sécurité informatique : les données et leur difficile qualification. Le second renvoie au processus même de sécurisation. Jamais uniquement "technique", nous verrons qu'il implique une solidarité entre hommes et machines dont l'équilibrage est particulièrement délicat.

Qualifier des données

Dans les entreprises, on ne trouve personne pour critiquer l'idée qu'il faille sécuriser les accès au réseau, les données électroniques et le matériel lui-même. La sécurité informatique est un bien en soi qui n'est jamais remis en question en tant que tel dans les entretiens. Toutefois, parce qu'ils projettent une exigence de réflexivité, les entretiens donnent aussi à voir des moments de doute et de remises en question. Durant l'enquête, cette réflexivité a essentiellement porté sur la nature des documents qu'il était question de « sécuriser ». Plusieurs questions apparaissaient au fur et à mesure de l'entretien : qu'ont ces données de véritablement sensible ? En quoi sont-elles confidentielles ? Qu'est-ce que leur diffusion, ou leur perte, représenterait pour l'activité de la personne, de son groupe de travail, voire de son entreprise ? Les réponses à ces questions sont en général surprenantes au regard de tous les arguments qui avaient été employés jusque là pour défendre ce qui a été présenté comme les impératifs de la sécurité informatique. Une conclusion générale s'impose à tous : les données qui sont en cause ne sont « pas si sensibles que ça ». Dans le pire des cas, leur disparition, leur corruption ou leur divulgation, ne provoquerait pas de nuisances irréversibles...

Les arguments qui accompagnent ce mouvement réflexif, tenus par des utilisateurs "ordinaires", sont un matériau de recherche riche. Ils montrent d'abord ce qui est souvent un angle mort de la sécurité informatique : l'importance de définir la valeur des données produites, hébergées, ou simplement circulant dans l'entreprise. Ils offrent ensuite des pistes de réflexions utiles : ils montrent qu'il existe bel et bien un vaste pan de documents qui peuvent être jugés comme "peu sensibles" et donnent à voir les éléments sur lesquels s'appuie cette (dis)qualification. D'autre part, dans le mouvement inverse, ils permettent d'isoler quelques critères de la valeur des données, qui renvoient directement aux activités de l'entreprise et aux fonctions des personnes concernées.

Des données sans valeur ?

Lorsque les personnes interrogées affirment que leurs données ne méritent finalement pas l'attirail sécuritaire dont elles font l'objet, elles se réfèrent essentiellement à deux risques bien connus des responsable de la sécurité informatique : la perte et le vol. À leurs yeux donc, perdre certains documents (à l'occasion d'une panne d'ordinateur par exemple), ou les voir entre les mains de la concurrence, ne constituent pas un drame irrémédiable. Comment expliquent-ils cela ? Deux arguments sont centraux : le premier souligne les liens entre données et contexte de l'activité, le second rappelle les opportunités que représente l'importante circulation et les incessantes duplications auquel oblige le travail collectif quotidien.

Des documents qui ne valent rien "seuls"

Lorsque les personnes d'affirment que le vol ou le piratage de leur ordinateur par des concurrents ne représente pas un risque gigantesque, elles mettent principalement en scène l'inutilité effective des données "brutes" pour leurs concurrents : la plupart des données

---

entretiens approfondis ont été effectués dans 43 entreprises (une heure trente en moyenne), avec 17 responsables informatiques et 26 utilisateurs finaux.

n'existent pas d'elles-mêmes et ne valent pas grand chose toutes seules. Les concurrents auraient beau s'en saisir, ils n'auraient pas à leur disposition l'expérience des situations, ni la connaissance interpersonnelle des clients, ni les savoirs accumulés nécessaires à leur compréhension. La valeur professionnelle des informations n'est donc pas contenue dans les seuls écrits électroniques : elle est le fruit de l'encastrement fort entre la plupart des données et l'activité qui les contextualise et les historicise. Parce qu'elle est située, elle n'est pas susceptible d'être "volée" ou "espionnée".

Des écrits distribués

Une autre dimension est mise en avant dans les entretiens pour expliquer la faible gravité que constitue la disparition de certaines informations. Il s'agit généralement de souligner le très faible nombre de documents qui sont uniques au sein de l'entreprise.

L'importance que prennent aujourd'hui les formes de coopération dans le travail, associée à l'essor des moyens techniques de circulation de l'information sont pointés comme les conditions "naturelles" d'un régime de la duplication généralisée qui assure une forme de pérennité distribuée à la grande majorité des données produites et échangées. Les échanges entre collègues, avec la hiérarchie, les prestataires ou les clients installent de fait une quasi-impossibilité de véritablement perdre ces données. C'est moins ici la nature de certaines données qui est mise en avant que les conditions contemporaines de travail au centre desquelles se trouvent la communication et le travail relationnel (networking), comme l'ont montré L. Boltanski et È Chiapello[3], ou encore B. Nardi et S. Whittaker[4].

Quelques dimensions de la valeur propre des écrits électroniques

Une fois détaillées les raisons qui permettent d'écarter un très grand nombre de données des risques réels de confidentialité et de destruction, on peut s'arrêter sur les quelques cas où la question de la valeur des données est abordée en positif. Apparaissent alors des figures de données "sensibles" qui peuvent constituer des points de repère utiles dans l'exercice de qualification qui semble incontournable à la mise en place de solutions sécuritaires pertinentes.

Écrits stratégiques et confidentialité à court terme

Les documents qui sont le plus facilement qualifiés de sensibles face aux menaces électroniques sont les documents "stratégiques". Ceux-ci sont présentés comme des éléments importants de la marche de l'entreprise : ils enregistrent et établissent des décisions majeures ; ils détaillent les différents éléments des projets... Mais ce qui fonde la valeur des données est moins leur capacité à accompagner le processus organisationnel que le fait qu'ils représentent une part de l'activité qui ne doit pas être divulguée sur les marchés.

La valeur "stratégique" est essentiellement concurrentielle. Les données comptent parce que les informations qu'elles contiennent ne doivent pas tomber entre les mains d'entreprises qui pourraient anticiper (et donc contrer) les "coups" de l'organisation concernée. La valeur de ces documents est donc affaire de cadrage temporel. Elle s'inscrit dans les rythmes des marchés : leur protection est considérée comme une condition essentielle pour la compétitivité.

Innovation, code et « patrimoine »

Dans les secteurs innovants, les personnes mettent en avant une valeur sensiblement différente, qui prend plutôt une forme patrimoniale. Les écrits dont il est question ne sont pas ici des points d'appuis pour l'action de l'organisation : ils en sont le produit même. Les

[3] Boltanski, L. & Chiapello, È. (1999). *Le nouvel esprit du capitalisme.* Paris, Gallimard.

[4] Nardi, B.A. & Whittaker, S. (2002). « NetWORKers and their Activity in Intensional Networks », *CSCW* 11 (1-2), p. 205-242.

documents sont une partie constitutive des “biens” (dans le sens où l’entend M. Callon[5]) que l’entreprise met sur le marché, par exemple le code informatique intégrée dans un décodeur audiovisuel ou les équations d’un modèle économique complexe de gestion des transports urbains.

Du coup, la valeur des données n’est pas seulement attachée à la question de la confidentialité : elle renvoie aussi aux risques de perte et de destruction. Les enjeux de leur stockage et de leur sauvegarde récurrente sont immenses. Enfin, cela se traduit par une définition très précise de la valeur des informations mises en formes par ces données. Alors que la plupart des évaluations pessimistes qui cherchent à mesurer les pertes que représenterait l’éventualité d’une panne d’un disque dur dont la sauvegarde n’est pas à jour prennent la forme d’heures de travail, la perte de données “patrimoniales” est directement traduite sous la forme d’un prix clairement établi.

Documents internes, ressources humaines et vie privée

Une troisième forme de valeur peut être repérée à l’intérieur même des entreprises : celle qui est attribuée à toutes les informations qui ont à voir avec l’activité de gestion des ressources humaines. Le risque qui est pointé ici est celui de l’espionnage interne, bien plus que concurrentiel.

Ces documents sont considérés comme particulièrement sensibles de deux points de vue. D’un côté, ils contiennent des informations personnelles, dont la circulation mettrait à mal de nombreux principes de la protection de la vie privée. De l’autre, ils peuvent porter des informations qui donnent à voir des mécanismes décisionnels de l’action managériale (montant des primes, augmentations, etc.). Ils sont donc susceptibles de constituer pour les syndicats par exemple des moyens de pression ou de négociation dont on préfère qu’ils soient dépourvus.

Traces et illégalité

Au cours de certains entretiens, d’autres types de données sont apparus comme particulièrement sensibles. Elles n’étaient pas directement désignées, ni explicitement qualifiées. Elles constituent pourtant un pan entier des informations que les entreprises cherchent à contenir au maximum : il s’agit des données qui témoignent d’une manière ou d’une autre d’activités répréhensibles, voire illégales.

Les affaires qui mettent en cause des fichiers électroniques constitués illégalement (par exemple parce qu’ils contiennent des critères de discrimination à l’embauche), ou qui se saisissent de traces d’échanges électroniques pour fonder des accusations de tous ordres font souvent grand bruit dans l’espace médiatique. Elles montrent que la divulgation de certaines données très spécifiques peut nuire au fonctionnement d’une entreprise, l’obligeant, ainsi que certains de ses employés et dirigeants, à répondre devant la justice. La valeur de tels documents relève d’une confidentialité qui déborde largement le paysage concurrentiel. Cette valeur “juridique” est évidemment très difficile à appréhender et ne peut faire l’objet d’une qualification frontale. On peut cependant faire l’hypothèse qu’elle pèse de manière importante dans certains secteurs d’activité et que la frontière qui la sépare du caractère stratégique de certaines informations n’est pas complètement étanche.

Les données des autres

Enfin, une dimension essentielle apparaît à l’issue de cette enquête : l’attention particulière que les personnes accordent aux données qui ne leur appartiennent pas et qui leur ont été confiées. Dès lors que l’on possède des informations qui appartiennent à d’autres, le processus parfois complexe de qualification des données pour définir leur valeur et l’attention sécuritaire qu’elles méritent semble joué d’avance. Le simple fait d’être la propriété d’un client ou d’un partenaire suffit à désigner les documents comme éminemment

[5] Callon, M., Meadel, C. & Rabeharisoa, V. (2000). « L'économie des qualités », *Politix* 13 (52), p. 211-239.

sensibles, à la fois face aux risques de fuite et à ceux de destruction. Cette valeur est d'autant plus grande qu'elle implique la responsabilité de l'entreprise qui les manipule et les fait circuler. Les perdre ou en rendre la fuite possible est non seulement perçu comme un risque opérationnel concret, mais aussi comme la mise à mal d'un engagement (parfois contractuellement encadré) de l'entreprise.

Associer des hommes et des machines

Mais la sécurité informatique n'est pas qu'affaire de données, loin de là. Il suffit de se plonger dans la première revue spécialisée pour se rendre compte que deux grandes catégories d'"acteurs" se partagent l'essentiel des préoccupations : les machines d'une part (matérielles ou logicielles, les technologies sécuritaires ne cessent d'évoluer), les hommes d'autres part (ces fameux "usagers" dont on ne cesse à longueur d'articles de stigmatiser les comportements, voire l'inconscience). Dans les entreprises, on trouve aussi cette partition, mais sous un angle moins dichotomique. Il ne s'agit plus de vanter les mérites des premières et de mettre en lumière les faiblesses des seconds, mais plutôt de construire une solidarité sociotechnique en définissant, et en négociant, les places de chacun. Deux dimensions apparaissent centrales dans la mise en œuvre délicate de cette équilibre homme/machine.

Le poids humain de la sécurité

Au fil de l'installation de nouvelles applications, de nouvelles fonctionnalités dans les systèmes d'information, les manipulations qui sont demandées aux utilisateurs se complexifient. Parmi celles qui concernent directement la sécurité, la saisie (et donc la mémorisation et parfois la création répétée) de mots de passe tient une place primordiale. Ces opérations constituent une forme de participation assez forte de l'usager à la politique de sécurité. Or, avec la complexification des systèmes, cette charge est de plus en plus lourde. Le nombre d'identifiants augmente, leur forme se complique et le rythme de leurs changements s'accélère. Cela donne lieu une véritable saturation et, comme dans d'autres dimensions du travail contemporain[6], les usagers deviennent de véritables centres individuels de traitement et de gestion de l'information.

Face à cette pression qui semble atteindre les limites de la mémoire « interne » des personnes, les responsables informatiques voient se multiplier les stratégies qui visent, pour les usagers, à s'affranchir d'une partie du coût cognitif que représente la gestion des identifiants. Cela passe généralement par la mobilisation d'artefacts mémoriels plus ou moins sophistiqués. Une récente enquête de *Nucleus Research and KnowledgeStorm* (2006) affirme ainsi qu'un employé sur trois note ses mots de passe sur un support externe, ce qui est clairement présenté comme une hérésie.

À bien des égards, du point de vue des prescripteurs et dans la presse spécialisée, la gestion des mots de passe représente ainsi le talon d'Achille des politiques sécuritaires, au centre des incriminations régulières de l'usager, considéré par beaucoup comme le "maillon faible" de la chaîne sociotechnique de la sécurité informatique. En notant ses identifiants sur papier ou en les enregistrant dans un fichier texte, celui-ci rompt la chaîne et réduit à néant l'effort de tous ces autres composants, humains ou techniques.

Mais la figure de l'usager inconscient associée à ces critiques doit être nuancée. Ce problème est loin de laisser indifférent les utilisateurs sur qui pèse la charge cognitive et il y a une forte culpabilité des personnes qui y sont confrontées. On rencontre ainsi un véritable souci sécuritaire dans les pratiques associées à l'allègement du coût de mémorisation des identifiants. Les solutions sont différentes, mais répondent toutes à une volonté de reconstituer un chaînon sécuritaire que chacun sait fragilisé par l'impossibilité de garder ces codes en tête.

[6] Stinchcombe, A. (1990). *Information and Organization.* Berkeley, University of California Press.

Par ailleurs, si ces pratiques sont généralement fortement dénigrées par les prescripteurs, tous ne sont pas dans une position de stigmatisation systématique des utilisateurs. Il est assez commun pour les premiers de comprendre la charge que représente cette gestion des identifiants et de souligner que la "nature humaine" ne peut pas être changée à ce point-là. Dans certaines entreprises rencontrées, on trouve ainsi des projets, voire des systèmes déjà installés, qui visent à repenser les modalités d'authentification dans un but d'allègement, et donc de renforcement de la sécurité. Ces stratégies s'appuient sur une idée simple : ne pas surcharger la "ête" des usagers, c'est ne pas les pousser à rompre la chaîne sécuritaire en notant leurs identifiants n'importe où. Cela passe généralement par la mise en pace d'un identifiant unique qui déclenche une couche logicielle de gestion des identifiants spécifiques. Une des entreprises a poussé cette logique en adoptant un système de carte à puce qui regroupe tous les identifiants de la personne, sans que sa mémoire ne soit jamais sollicitée...

Cette solution possède évidemment ses propres défauts (la paralysie en cas de perte), mais souligne l'enjeu qui consiste aujourd'hui à dépasser le registre de l'accusation des utilisateurs pour prendre au sérieux la surcharge cognitive que représente la gestion individuelle des identifiants. Plus généralement elle montre très clairement que l'élaboration de chaque maillon de la chaîne sécuritaire (ici celui de l'identification/authentification) est une question fortement politique, au cœur de laquelle se dessinent des jeux délicats d'équilibrage entre les machines et les hommes.

« Chacun son métier » Vs. « C'est l'affaire de tous »

Des appels alarmistes qui pointent du doigt l'inconscience des usagers jusqu'aux attitudes compréhensives des prescripteurs qui cherchent à prendre en considération les difficultés opérationnelles et cognitives des obligations sécuritaires, tout montre à quel point sécuriser veut aussi dire prendre position sur la nature et le degré d'enrôlement des utilisateurs. Une partie des entretiens apporte un éclairage spécifique sur cette dimension et donne à voir un véritable point de tension entre prescripteurs et utilisateurs. Non pas tant du côté de la conscience sécuritaire et des différentes formes de sensibilisation qu'elle nécessiterait que du côté de la participation effective à la politique de sécurité informatique.

Des usagers en retrait

Du côté des usagers, on repère une tendance chez certains à cantonner précisément le lieu des préoccupations sécuritaires aux services officiellement désignés. Il n'y a pas dans cette attitude un rejet des règles mises en place par les prescripteurs informatiques, mais plutôt une volonté de définir les contours de *métiers* distincts, aux préoccupations clairement réparties. Cette attitude s'affirme sur le registre de la confiance aveugle faite aux responsables informatiques. Une telle position tend à privilégier au maximum les solutions techniques automatisées qui inscrivent les règles dans des routines informatiques. L'engagement de l'utilisateur est alors minimal. Il peut s'appuyer sur des dispositifs constitués en boîtes noires, sans avoir à porter une part de la charge sécuritaire.

Plus généralement cette posture s'appuie aussi sur l'absence de compétences techniques qui permettraient de s'engager dans des opérations sécuritaires plus poussées. Le discours est doublé : non seulement "ce n'est pas mon métier", mais plus encore, "je n'y connais rien". Ce type d'argument traverse les toutes petites entreprises dont les principaux prescripteurs sont les prestataires de services informatiques, ou les opérateurs. On trouve là aussi une posture de désengagement (parfois subie) qui consiste à s'appuyer le plus possible sur les engagements de l'offreur, réputé connaître son métier.

Ces attitudes assez solidement argumentées lors des entretiens contrastent avec la posture largement partagée chez les prescripteurs qui consiste à insister sur la nécessité de mettre le "facteur humain" au centre des politique sécuritaires.

Prescription technique et investissements humains

C'est un allant de soi chez les prescripteurs : la chaîne sécuritaire est une chaîne *socio*technique. La sécurité purement technique, c'est-à-dire entièrement réalisée dans des scripts, est impensable. L'implication de tout le monde dans le processus est considérée comme la pierre de touche de la sécurité informatique. Cela se traduit par un grand nombre de stratégies d'enrôlement des usagers, qui vont au-delà des enjeux de sensibilisation et de communication. Par exemple, certains services délèguent entièrement des opérations sécuritaires telles que la sauvegarde. Cette stratégie est présentée comme un moyen de mettre les personnes "en face de leurs responsabilité" et de leur faire prendre conscience des risques informatiques en les y confrontant directement. Mais l'importance du "facteur humain" est parfois argumentée de manière beaucoup plus ambitieuse. Avoir conscience des problématiques de sécurité, comprendre les risques encourus ne doivent pas tant être des éléments auxquels sensibiliser, mais 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.

On le voit, les discours des uns et des autres sont radicalement opposés. Face à une véritable demande de désengagement, de discipline équipée et allégée par les dispositifs techniques, les propos des prescripteurs misent sur l'enrôlement fort de chacun. Il faut toutefois circonscrire l'espace de cette opposition : elle est essentiellement un problème de grande entreprise où la division du travail est importante et où chacun peut réellement revendiquer une posture de métier spécialisée et désengagée. Les petites entreprises donnent à voir des ambiances nettement différentes où chacun est naturellement impliqué dans les principes sécuritaires, notamment en ce qui concerne les données sensibles et les enjeux de confidentialité. La grande entreprise, qui plus est lorsqu'elle est distribuée sur plusieurs sites, se trouve dans une situation particulièrement sensible sur ce point. Non seulement, elle dispose d'outils sophistiqués et de services importants qui peuvent développer (et développent la plupart du temps) des solutions sécuritaires automatisées et transparentes, mais elle est confrontée à l'éclatement physique et moral de ses employés. Elle se trouve donc en situation de proposer des solutions d'allégement cognitif ou opérationnel qui facilitent le désengagement des usagers, sans disposer de véritables outils d'enrôlement des personnes dans les politiques sécuritaires.

La tension mise en lumière ici entre la position des usagers et celle des prescripteurs est donc fort différente de celle qui apparaît dans les discours généralistes. En tout cas, elle se présente sous un autre jour. Nous n'avons pas d'un côté des utilisateurs inconscients qui ne se préoccupent pas de sécurité et sont réticents à toutes règles techniques, et de l'autre des responsables informatiques tyranniques qui ne cherchent qu'à contraindre et contrôler les premiers. D'un point de vue général, les positions vont même à l'encontre des hypothèses traditionnelles. Les techniciens ne défendent aucunement leur pré carré professionnel, purement techniciste, face aux non-initiés. De la même manière, les usagers ne plaident pas ici pour une humanisation ou un ré-enchantement de la technique. La place et le rôle des entités qui composent la chaîne sécuritaire ne vont pas de soi et les processus d'enrôlement et d'engagement sont multilatéraux.

Conclusion

La mise en place de principes et de solutions sécuritaires dans une entreprise relève d'une dynamique éminemment politique. Qu'il s'agisse de qualifier ce qui doit être securisé, ou de définir l'équilibre des forces techniques et humaines, rien n'est fixé d'avance. Dans ce mouvement, il n'y a ni recettes, ni formules toutes prêtes. Il faut passer par des négociations,

des “régulations conjointes”[7], parfois des controverses, qui ponctuent un long travail de convention.

Plutôt que de le rabattre sur des jeux de pouvoir ou d’en réduire la portée par un discours systématiquement critique, ce travail peut être appréhendé comme un cas exemplaire des nombreuses arènes qui composent la “société de l’information”. Les débats qui le nourrissent apparaissent alors dans leur consistance anthropologique. L’élaboration de chaque maillon de la chaîne sociotechnique dont nous avons vu quelques figures ici nécessite de définir en commun une forme de solidarité spécifique entre les entités qui la composent (personnes, services, objets techniques, logiciels, etc.). Dans ce processus, ni les machines ni les hommes ne sont dotés de places figées, qui correspondraient à leur hypothétique nature. Chaque régime de solidarité au sein de la chaîne est autant un point d’appui à l’action sécuritaire qu’un de ses résultats.

Le type d’enquête présenté ici n’offre qu’un aperçu rapide des manières de s’accorder sur ces places et ces rôles dans des situations concrètes. Pour saisir l’épaisseur pragmatique de tels agencements et continuer d’explorer la variété des montages auxquels ils aboutissent, il devra laisser la place à des études plus approfondies, prenant par exemple la forme de suivis monographiques de projets. C’est seulement dans ce deuxième mouvement empirique que la diversité des formes sécuritaires de la solidarité sociotechnique pourra être pleinement documentée.

Références

Boltanski, L. & Chiapello, È. (1999). *Le nouvel esprit du capitalisme.* Paris, Gallimard.

Callon, M., Meadel, C. & Rabeharisoa, V. (2000). « L'économie des qualités », *Politix* 13 (52), p. 211-239.

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

Nardi, B.A. & Whittaker, S. (2002). « NetWORKers and their Activity in Intensional Networks », *CSCW* 11 (1-2), p. 205-242.

Reynaud, J.-D. (1979). « Conflit et régulation sociale. Esquisse d'une théorie de la régulation conjointe », *Revue française de sociologie* 20 (2), p. 367-376.

Stinchcombe, A. (1990). *Information and Organization.* Berkeley, University of California Press.

[7] Reynaud, J.-D. (1979). « Conflit et régulation sociale. Esquisse d'une théorie de la régulation conjointe », *Revue française de sociologie* 20 (2), p. 367-376.