La prescription de la sécurité informatique en entreprise. Figures de la solidarité sociotechnique

Jérôme Denis

La prescription de la sécurité informatique en entreprise
Figures de la solidarité sociotechnique

Jérôme DENIS

TELECOM ParisTech
Département Sciences Économiques et Sociales
46, rue Barrault
F-75634 Paris Cedex 13
01 45 81 76 11
http://ses.enst.fr/denis

Résumé

À partir d'une enquête par entretiens, cet article cherche à sortir du cadre des débats médiatiques pour comprendre les conditions concrètes des politiques sécuritaires en entreprise et les arguments qui les fondent. La prescription de la sécurité informatique y est appréhendée comme processus d'élaboration d'une chaîne sociotechnique qui associe dans une marche commune des personnes et des équipements variés (postes informatiques, logiciels, serveurs, câbles...). Mais les négociations et les ajustements qui accompagnent ce travail ne sont pas univoques. L'établissement de chaque maillon de la chaîne sécuritaire donne lieu à des formes de solidarité sociotechnique spécifiques. L'analyse porte plus particulièrement sur deux dimensions de ce travail d'ajustement : la difficile articulation des règles techniques et managériales (et donc l'harmonisation des services internes qui les produisent), et l'équilibrage subtil entre actions humaines et automatismes techniques.

Mots clés

Sécurité informatique - Prescription - Usages - Solidarité sociotechnique

Denis, J., 2007. « La prescription de la sécurité informatique en entreprises. Figures de la solidarité sociotechnique », *in* Carré, D. (dir.), *14ème Colloque du CREIS. De l'insécurité numérique à la vulnérabilité de la société*, Paris, CREIS.

Pour un regard symétrique : ce que sécuriser veut dire

Depuis plusieurs années, les manières d'étudier les nouvelles technologies et notamment leurs usages professionnels se sont transformées. À côté d'une posture exclusivement critique, qui tend parfois à distribuer les rôles et les rapports de force avant toute enquête, une perspective pragmatique s'est développée qui cherche à comprendre les usages en situation en s'appuyant sur une documentation détaillée et symétrique des personnes, des technologies, des discours et des activités qui y sont engagés. Le but de cette posture est de laisser aux acteurs la main sur les définitions du monde dans lesquels ils sont engagés (Callon, 1986), afin d'observer avec un même intérêt ce qui est critiqué par les uns et défendu par les autres, et finalement de saisir les modalités concrètes de l'accord et du désaccord.

Sécurité informatique et chaînes sociotechniques

Dans ce mouvement, de nombreuses recherches ont montré l'importance des processus de constitution et de stabilisation de chaînes sociotechniques : elles dessinent une vue dynamique du social et de la société focalisée sur les formes d'association entre des hommes et des machines (et plus généralement des « non-humains »)[1]. L'enjeu est alors d'une part d'étudier les controverses et de décrire les opérations qui aboutissent à stabiliser cette solidarité sociotechnique, et d'autre part de comprendre le plus finement les dispositifs et agencements auxquels elle donne naissance.

La sécurité informatique est un objet qui se porte particulièrement bien à ce type de questionnement. Elle est aujourd'hui une des dimensions essentielles de la « société de l'information » et se trouve donc au cœur d'un vaste discours critique, prise dans de nombreuses controverses dont l'éventail s'étend de la transformation de l'espace public à la protection de la vie privée en passant par le renouvellement des formes de commerce, de travail ou encore d'administration (Chateauraynaud & Trabal, 2003). Plus encore, la mise en œuvre de politiques sécuritaires dans les entreprises apparaît comme un terrain d'investigations prometteur. Encore très peu étudié, il est à la croisée d'enjeux technologiques « généralistes » et de problématiques spécifiquement professionnelles telles que les rapports entre nouvelles technologies et productivité, la transformation des modes de travail (notamment liées aux possibilités accrues de travail à distance) ou encore les liens entre informatique, prescription et contrôle hiérarchique.

Insécurité numérique : à qui la faute ?

Tant sur le versant grand public que sur celui des entreprises, une large part des discours dans les médias spécialisés porte explicitement la volonté de transformer la nature des liens qu'entretiennent les humains et les machines (majoritairement les ordinateurs et les serveurs) au nom des exigences sécuritaires. Cette volonté passe par une stigmatisation assumée des « utilisateurs », qu'ils soient patrons ou employés dans le cas qui nous intéresse. Ceux-ci sont généralement décrits comme « inconscients » et la nécessité de les encadrer, et plus encore de les éduquer, est un leitmotiv qui traverse de très nombreuses publications. À l'inverse, les discours critiques pointent du doigt les technologies elles-mêmes et leurs promoteurs. Dans une posture de dévoilement, ils soulignent les mécanismes et les enjeux « cachés » derrière l'adoption massive des nouvelles technologies et d'Internet et cherchent à repositionner devant la scène les usagers et leurs besoins « réels », voire leurs droits.

---

[1] En France, l'ouvrage de N. Dodier (1995) exemplaire de cette position. Dans une perspective proche, mais plus générale, le projet de B. Latour tel qu'il l'a récemment synthétisé (Latour, 2006) participe de cette même ambition théorique et empirique.

La critique et les médias spécialisés partagent donc plus de choses qu'on ne l'imagine à première vue. Ils s'accordent d'abord sur un constat alarmiste qui souligne le caractère contradictoire du développement considérable des technologies informatiques et pointe le profond paradoxe de notre société de l'information. 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. Forts de ce constat de vulnérabilité, les deux discours adoptent ensuite une posture qui obéit à une même logique : l'imputation d'une faute clairement identifiable. Qu'il s'agisse des technologies et de leur promoteurs d'un côté, ou des usagers de l'autre, la mécanique argumentative est la même. Elle consiste à plaider pour un rééquilibrage de la balance sociotechnique selon que l'on juge le poids des uns et des autres trop grand ou trop faible.

Les conditions effectives de la sécurité informatique

S'ils invitent naturellement à la curiosité du chercheur, ces débats n'offrent qu'une vision très restreinte de la question sécuritaire. Ils ne donnent rien à voir, notamment, de ce qui se passe effectivement dans une entreprise ou une organisation lorsqu'une politique sécuritaire est mise en place. Or, en situation, les tensions et les débats qui se créent autour des jeux d'équilibrage entre responsabilisation des usagers et toute puissance des machines sont beaucoup plus complexes. Pour comprendre la place qu'ils tiennent et les enjeux qu'ils cristallisent dans les entreprises, il faut se pencher sur des cas précis, et adopter un point de vue symétrique : d'un côté, en affinant l'étude du point de vue des prescripteurs de sécurité et de l'autre, en interrogeant celui des usagers eux-mêmes. Cette posture empirique est un moyen de décaler le regard analytique en passant du régime des discours de justification où l'enjeu est de produire des montées en généralité qui fondent les arguments des uns et des autres, vers un régime d'accords et de désaccords où il n'est pas interdit de revendiquer une certaine forme de généralité, mais où les actions et les discours sont toujours ancrés dans des épreuves de validité locales (Thévenot, 1990). Si la sécurité informatique semble être une préoccupation de plus en plus grande dans les entreprises, on peut ainsi se demander comment ce « souci » très général se traduit dans des pratiques concrètes, des dispositifs et des formes de communication en situation. Quelle(s) forme(s) prend cette prescription particulière, a priori essentiellement technique ? Comment s'en charge-t-on quotidiennement ? À quels usages effectifs donne-t-elle lieu ? Quels types de tensions soulèvent-elle ?

Ces questions sont vastes et les traiter complètement nécessiterait de longues investigations ethnographiques qui restent à mener. Plus modestement, je propose ici de tracer un certain nombre de pistes exploratoires pour comprendre comment le souci sécuritaire s'incarne et se discute dans les pratiques quotidiennes. Pour cela, je m'appuierai sur une enquête menée auprès de 43 entreprises, financée par le laboratoire SUSI de France Telecom R&D[2]. Celle-ci a consisté à effectuer des entretiens approfondis (une heure trente en moyenne) avec 17 responsables informatiques et 26 utilisateurs finaux. Cette méthode permet de prendre au sérieux les positions de chacun et de dépasser les antinomies trop évidentes entre prescription sécuritaire et activités ordinaires. Nous verrons au fil de cette communication que les places sont mouvantes et que la mise en œuvre d'une politique sécuritaire ne se réduit pas à l'opposition entre des usages prescrits d'un côté et du « braconnage » de l'autre.

[2] Cette enquête a été suivie par Emmanuel Kessous et réalisée avec l'aide de Damien Guillaume.

Je suivrai deux axes principaux afin de donner à voir les différentes facettes des politiques sécuritaires en entreprise. Dans un premier temps, je m'arrêterai sur les activités des prescripteurs eux-mêmes, en montrant que celles-ci ne se limitent pas à l'encadrement des seuls usagers, ni à un travail d'alignement de chacun sur leurs propres règles. Puis, en ajoutant au tableau les points de vue des usagers, je montrerai que leur soi-disant désengagement n'est pas si fort et qu'il existe malgré tout une certaine « demande » sécuritaire. À travers ces deux versants des politiques sécuritaires, nous verrons que la solidarité sociotechnique qu'il s'agit de tisser pour installer une sécurité acceptable n'est pas univoque et qu'elle repose sur des opérations spécifiques.

Agencement des prescripteurs, articulations des règles : quand la sécurité travaille l'organisation

Du côté du grand public, mais plus encore évidemment dans les entreprises, la sécurité informatique est avant tout affaire de prescription. Il s'agit pour certains acteurs de dire à d'autres ce qu'il faut faire, jusqu'à parfois les y contraindre d'une manière ou d'une autre. Mais cette prescription est bien particulière. Elles n'est pas assise sur des statuts organisationnels clairs. Les personnes qui en ont la charge dans les organisations (responsables informatique, administrateurs réseaux, voire explicitement « responsables de la sécurité informatique »...) ne sont pas liées par des rapports d'autorité aux usagers auxquels elles imposent des solutions techniques et dont elles encadrent certains comportements. Et par là même, la prescription de la sécurité informatique peut être considérée comme une prescription « concurrente » des instances prescriptives officielles, clairement identifiées comme telles dans les organigrammes. Cette posture prescriptive ambiguë constitue un premier objet d'analyse pour comprendre ce que sécuriser veut dire.

Depuis les travaux de M. Crozier et E. Friedberg, les analyses inspirées de la perspective stratégique nous ont habitués à voir dans les relations professionnelles, et notamment dans celles qu'entretiennent les services techniques avec le reste de l'entreprise, des luttes pour le pouvoir. En suivant cette veine, on pourrait sans doute réduire les liens qui unissent certains responsables informatiques à la ligne hiérarchique de leur entreprise à des jeux tactiques 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. Mais cela serait fortement dommageable. Il nous serait par exemple impossible de comprendre que les objectifs des uns et des autres ne sont pas *a priori* distincts. Plus encore, cela nous obligerait à ne pas véritablement écouter ce que nous racontent les interviewés et à écarter leurs arguments et leurs histoires au nom du dévoilement de leurs soi-disant arrières pensées machiavéliques. On l'aura compris, cette recherche n'est pas animée par ce genre d'ambition. Prenons donc au sérieux ce que les prescripteurs de sécurité nous racontent sur les rapports qu'ils entretiennent avec les différents autorités de l'organisation.

La première caractéristique de ces rapports est assez bien connue. Il semble que le bon fonctionnement d'une politique sécuritaire se mesure à la « normalité » des traitements que subit la hiérarchie. Si les managers et les hauts cadres obéissent aux mêmes règles de sécurité que les petits employés (changements de mot de passe, effectuations des mises à jour régulière, interdictions de surfer sur tel type de sites Web, etc.), alors l'entreprise a toutes les chances d'être à l'abri des principaux risques informatiques. Et cet aplatissement des hiérarchies devant les règles sécuritaires n'est pas tant une question de pouvoir qu'un principe de justice. On se trouve ici devant la volonté de constituer un « collectif d'égaux », dont l'épreuve principale est la « faveur » (Joseph, 2004). En témoignent les réactions de quelques responsables informatiques qui, soulignant la dimension contraignante de certaines de leurs règles, stigmatisent les passe-droit et autres dérogations qu'ils sont parfois obligés de donner au nom du seul statut de leurs bénéficiaires.

Mais nous n'avons là qu'un aperçu incomplet de la prescription sécuritaire : celui qui touche aux règles les plus « simples », dont le champ est finalement réduit. Une large part des politiques sécuritaires débordent de ce cadre, notamment dans les moyennes et grandes entreprises. C'est le cas de la gestion des droits d'accès au système d'information. Celle-ci est présentée par certains comme la clef de voûte de la sécurité informatique, primordiale tant pour garantir l'intégrité des données que pour assurer l'organisation du système d'informations tout entier et minimiser des risques d'espionnage interne. Or, cette gestion ne s'arrête pas à l'application de règles binaires où il s'agirait seulement d'autoriser certains à « entrer » et d'interdire aux autres. Il faut non seulement définir « où » chacun peut entrer, ce à quoi il a effectivement accès (quels dossiers, et quels fichiers dans le système d'informations) mais aussi définir ce qu'il aura le droit d'y faire (lire, copier, imprimer, modifier...).

> 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 et après mettre en place des outils ou les contrôles pour empêcher que… pour que la personne puisse faire vraiment ce qui est défini. (*Responsable informatique, énergie*)

On s'en doute, cet aspect est particulièrement complexe à mettre en œuvre. La difficulté ne vient pas de la technologie à déployer. Au final, il s'agit d'un système d'autorisation assez simple basé sur des profils que l'on attribue aux usagers (d'où son nom : *profiling*). La complexité réside bien plus dans l'intrication des niveaux organisationnels et techniques : dans bien des cas, mettre en œuvre des principes de *profiling*, c'est mettre le doigt dans un engrenage extrêmement délicat qui déborde les compétences techniques des services informatiques. Cela engage un véritable travail d'objectivation de structures organisationnelles que l'on tient généralement pour acquises, mais qui se dérobent à la moindre tentative de mise à plat. Pour attribuer des profils, il faut, avant d'attribuer des droits, répondre à des questions abyssales dans des grandes entreprises telles que « qui fait quoi ? » ou « qui est à l'intérieur de l'entreprise, qui est à l'extérieur ? ». 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 ici liées : à l'instar des démarches qualité, la politique sécuritaire se trouve en situation ici de faire *travailler* l'organisation (Cochoy et al., 1998).

Cette articulation des problématiques techniques et organisationnelles souligne par ailleurs l'enjeu qu'il y a pour certains responsables informatiques à enrôler les lignes hiérarchiques de l'entreprise sous une forme toute autre que la soumission aux règles qu'ils instaurent ou leur accompagnement par voie de communication interne. C'est le rôle et le statut même des prescripteurs techniques qui sont en jeu dans cet enrôlement. Il y a ainsi parmi les responsables de la sécurité un net refus à endosser des opérations qu'ils n'estiment pas de leur ressort. Dès lors qu'il s'agit d'activités totalement hybrides, comme le *profiling*, la hiérarchie doit à leurs yeux absolument s'engager et assumer sa part de prescription.

> 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 on est garants, on est les gendarmes, mais on n'est pas le prescripteur. (*Responsable informatique, énergie*).

Les pratiques de *profiling* mettent ainsi en lumière une autre forme de solidarité sociotechnique, qui s'ajoute à la seule figure de l'attachement/soumission souvent mise en avant par la critique. Au travail de sensibilisation (des usagers et de leur hiérarchie) s'ajoute la nécessité de monter de véritables « agencements organisationnels » (Girin, 1995) qui sont seuls capables d'inscrire les principes sécuritaires au cœur de l'entreprise. Dans ces agencements, les services informatiques, ou les responsables de la sécurité eux-mêmes lorsqu'ils existent, insistent pour « rester à leur place », c'est-à-dire ne pas prendre en

charge une prescription autre que technique. En délimitant ainsi leur champ d'activité, ils définissent en creux le rôle de la ligne hiérarchique dans la mise en œuvre des politiques sécuritaires. Celle-ci est invitée à prendre part à l'agencement en assurant la production et la circulation de règles organisationnelles pour la sécurité qui seront ensuite traduites en règles techniques par les services informatiques. C'est sur cette opération de traduction, et donc sur l'existence préalable des premières, que les secondes s'appuient pour *tenir* en tant que règles légitimes aux yeux de tous, et sortir du soupçon de l'*arbitraire technique* qui pèse invariablement sur les prescriptions informatiques. Ce chaînage de règles organisationnelles et techniques apparaît ainsi comme un moyen particulièrement puissant du *sensemaking* dont Weick (2001, p. 148-175) et d'autres (Orlikowski et al., 1995) ont souligné qu'il était un enjeu central dans les processus d'adoption des technologies dans les entreprises.

Sécurité et usages : des hommes ou des machines ?

Dès lors que l'on insiste sur les dimensions prescriptives du travail des responsables de la sécurité informatique, la question des contournements et des comportements non conformes des utilisateurs apparaît sous un jour nouveau. La sociologie du travail et des organisations, tout comme l'ergonomie, n'ont cessé de montrer qu'à côté du « travail prescrit » (celui des règles officielles et de l'encadrement) se déployait un « travail réel », véritable océan d'activités ad'hoc. Et les recherches sont innombrables qui ont montré que ces activités qui ne suivent pas les règles à la lettre sont essentielles à la bonne marche effective de la production (Daniellou et al., 1983 ; de Terssac, 1992 ; Clot, 1998). Par ailleurs N. Dodier a montré que le contournement des règles sécuritaires pouvait relever non plus d'une « efficacité malgré tout », mais d'une mise en scène de soi et de sa virtuosité (Dodier, 1996). Qu'en est-il des usages « réels » des équipements informatiques ? Quels types de tensions les entretiens donnent-ils à voir ?

Nous l'avons vu, les discours médiatiques, dans la presse grand public comme dans la presse spécialisée, mettent en scène une rupture profonde entre enjeux sécuritaires et préoccupations ordinaires des usagers. D'un point de vue général, cette enquête laisse voir que la rupture n'est pas si flagrante. Dans la plupart des cas, prescripteurs et usagers semblent engagés dans des postures plutôt conciliantes où il s'agit avant tout de « faire avec » l'autre : faire avec les règles d'un côté, faire avec la nature humaine de l'autre. On trouve pourtant de véritables points de tension entre les prescriptions et les usages, bien qu'ils ne relèvent qu'indirectement d'une problématique de type prescrit/ réel. Parce que s'y posent — parfois explicitement — la question de l'équilibre entre action humaine et action technique, l'étude de ces tensions vient enrichir l'analyse de la solidarité sociotechnique qui fonde les politiques sécuritaires.

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. Il ne s'agit plus de « faire attention » à sa machine, ou d'ajuster ses comportements dans un régime de prévention plus ou moins rigide, mais de prendre directement en charge la part de la sécurité qui consiste à authentifier les personnes. 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 (Stinchcombe, 1990), les usagers deviennent de véritables centres individuels de traitement et de gestion de l'information.

> Alors les codes, c'est pareil. Il y a des codes, ça me fait rire *(rires).* Chez nous, les codes c'est super compliqué, justement. Même moi au niveau des codes, je suis obligé d'avoir un email perso où je mets tous les codes. C'est-à-dire que… je ne me souviens pas en fait. Il y a tellement de codes… Que effectivement je peux pas les retenir quoi. Mais sinon, effectivement, pour la base de connaissances, il faut un login et un *password*. Pour le système d'exploitation, il faut un login et un *password*. Pour la base d'archives des contrats, il faut un login et un *password*, pour d'autres espaces, il faut un login et un *password*. J'ai tellement de… et c'est pas les même. Alors des fois, c'est les mêmes. On peut utiliser le même, mais des fois, c'est pas les mêmes parce que justement, ce qui se passe, c'est qu'il y a une politique chez nous de changer les logins et les *password* régulièrement… Et qui n'ont pas les mêmes dates entre les différentes applications. Alors, du coup vous êtes là à changer votre login de votre système, votre identifiant et votre système d'exploitation mais celui de la base de connaissances est changé dans un mois. Donc vous laissez et vous vous retrouvez en fait à gérer vous-même une petite base de données... *(Responsable clientèle, Services Web)*

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[3], 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 refusant de prendre encharge sa part du « travail », et 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 pèsent 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. Un premier moyen consiste par exemple à s'appuyer sur un support papier que l'on cherche à « bien » ranger.

> Le problème c'est que le mot de passe comme on le change quand même assez souvent il faut le noter quelque part. Alors après vous oubliez où vous l'avez noté parce qu'on n'est pas vraiment tous très ordonné Moi ça m'est arrivé effectivement de le perdre et de ne plus avoir en tête et de le confondre avec d'autres mots de passe parce que j'ai aussi plein d'autres sur internet, plein de machins pour lesquels il faut des mots de passe. C'est vrai qu'il y a une réelle difficulté de gestion des mots de passe. (*Vous les notez dans l'ordinateur ?*) Ah non sur un papier. Mais la difficulté elle est là : où je le note ? Souvent je fais un papier et je me dis « Tiens je vais le mettre dans la poche de mon cartable » mais ce n'est pas forcément sécurisé. Alors souvent je le mets dans un des tiroirs de mon bureau. J'écris un papier avec mes mots de passe et je les mets dans un des tiroirs de mon bureau. *(Commercial, SSII).*

Une autre stratégie cherche à jouer sur la surcharge des informations présentes sur un ordinateur, et « noyer » un fichier contenant les identifiants en clair dans la masse des documents bureautiques disponibles. C'est le cas d'une personne qui « cache » ses codes dans un message électronique camouflé dans la masse de ses messages personnels.

---

[3]. Source : http://news.com.com/

Enfin, on trouve aussi des personnes qui reconstituent le maillon sécuritaire en s'appuyant sur des technologies « approuvées » par les services sécuritaires, puisque mises en place par elles pour d'autres types de données. C'est le cas du cryptage du fichier contenant la liste des mots de passe, et de sa mise en « lieu sûr » : sur le serveur interne.

> J'en ai beaucoup [des identifiants]. Oui. Justement, pour faire ça, j'utilise après des fichiers cryptés avec tous mes mots de passe dedans. Que j'ai sur le serveur. Je ne l'ai pas à distance. Je les ai sur le serveur. Mais pas dans la machine. Je les mets justement sur le serveur de l'entreprise, ce qui me permet au cas où je me ferais voler le PC, eh bien, il n'y a rien sur le PC. Et que je ne peux uniquement accéder que quand je suis connecté. (*Ingénieur commercial, télécommunications*).

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 « tête » 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...

> Nous, on a choisi justement de crypter ça via des cartes à puce. Typiquement un collaborateur qui part avec son ordinateur portable, il part également avec sa carte à puce qui est protégée comme le système de carte bleue avec un système à quatre chiffres qui lui permet… dessus le collaborateur en fait ne connaît plus ses logins et ses mots de passe. Ils sont stockés et cryptés directement sur la carte à puce. Lui, a juste à utiliser sa carte à puce, à rentrer son code pin et après la carte à puce en fait remplit lui-même les champs où il y a demandé Login, mot de passe. […] Alors, d'une part c'est pour simplifier, voilà. C'est déjà pour éviter clairement d'avoir le *post-it* dans sa mallette du portable. Parce que si jamais il se fait piquer sa mallette et que dedans il y a la feuille, « alors mon login pour Lotus notes, c'est ça » et « mon login pour ci, c'est ça », là, le niveau de sécurité est de zéro. […] Et l'avantage c'est la simplification puisqu'on a quand même X applicatifs qui tournent ils n'ont plus aucun login et mot de passe à retenir. Puisque chaque applicatif a son login, a son mot de passe, tout est stocké sur la carte à puce. Qu'à partir du moment où il est authentifié avec sa carte à puce, il a accès à tous ces applicatifs sans avoir à ressaisir ses logins et ses mots de passe. *(Responsable Réseau et Sécurité informatique, Assurances).*

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) 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 »*

Le dernier point soulevé ne se réduit pas à la dimension contraignante de la sécurité et aux jeux d'engagement/désengagement que chacun déploierait pour se plier ou échapper à cette contrainte. Il soulève un enjeu beaucoup plus vaste : celui de la forme d'engagement des utilisateurs dans la politique sécuritaire. 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.

> Il y a des sécurités c'est sûr à tire-larigot. Mais nous, on n'est pas au courant, on est… chacun a son métier. C'est-à-dire nous, on est commercial, on nous communique des outils pour communiquer, pour améliorer notre quotidien, mais je veux dire, les problèmes d'informatique, bon, ça me passe au-dessus de moi. Je veux dire, c'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).*

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.

> Non, je ne m'occupe de rien. Moi je fais mon boulot, sachant que les données sensibles, j'appuie sur un bouton et pff. C'est tout. C'est la seule chose que je fais. Tout le reste, c'est ni plus ni moins que mon boulot, c'est-à-dire rédiger des rapports, faire des calculs, des machins. Le reste, je ne m'occupe de rien. Il y a des gens, encore une fois, compétents dans ce domaine, bien plus que moi, d'ailleurs. […] 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. Donc ça, c'est pas trop dur. Pas trop astreignant. *(Ingénieur R&D, Aéronautique).*

Plus généralement cette posture de cadrage 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.

> Mais moi, je ne m'en angoisse pas parce que j'ai les produits pour me protéger et puis par ailleurs, je fais confiance aux constructeurs à partir de l'instant où ils vous disent « Bon, ben, la Livebox »… Quand on m'a dit qu'il y avait un Firewall derrière et ben, le Firewall de Microsoft, je l'ai débranché en fait… Et puis le Firewall de mon antivirus Norton, il est pas non plus actif. Parce que je sais qu'il y a celui-là, qui est actif. Et comme chez Wanadoo, ils m'ont dit : « Il faut que les deux autres ne soient pas actifs sinon, ça crée des problèmes »… Ce qui a été le cas, justement, pendant un moment… donc, aujourd'hui, j'ai celui-là qui marche… Le Firewall de la Livebox. Je fais confiance à la technique. J'ai… on n'a pas le choix de toute manière. *(Ingénieur conseil libéral).*

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 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 que doivent jouer les 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, je dirai, 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 des usagers, qui vont au-delà des enjeux de sensibilisation et de communication. Par exemple, certains services délèguent entièrement certaines opérations sécuritaires telles que la sauvegarde. Cette stratégie est présenté 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.

> 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, d'abord ces choses-là sont en petit nombre. […] 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 dont qu'ils détiennent. *(Administrateur réseau, transports).*

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. Cela est plus fort encore lorsque l'entreprise est dans le secteur des nouvelles technologies.

> Typiquement, les gens ne s'installent aucun produit qui ne soit pas validé par la DSI. C'est-à-dire qu'implicitement, je pense qu'on a nous, cette chance, que les gens sont des utilisateurs relativement responsables. Ils savent eux-mêmes que si jamais il y a un problème de sécurité dans l'entreprise, c'est aussi leur vie dans l'entreprise, qui risque d'en être atteinte. Je veux dire, on n'a pas une population de gens qui passeront trois heures par jour sur Internet, dans les forums où chacun va aller distribuer son adresse mail à la terre entière sur les forums et va se retrouver à recevoir 25 millions de mails par jour, en *spams* et *spyware*. *(DSI, SSII et audiovisuel).*

La grande entreprise, qui plus est lorsqu'elle est distribuée sur plusieurs sites, se trouve donc 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. En focalisant l'analyse sur la dimension prescriptive, j'espère avoir montré que pour les personnes elles-mêmes engagées dans cette dynamique, l'enjeu est de constituer une chaîne sociotechnique composée de maillons dont les modalités d'attachement sont acceptables. Dans ce mouvement, il n'y a ni recettes, ni formules toutes prêtes. Il faut passer par des négociations, des « régulations conjointes » (Reynaud, 1979), parfois des controverses, qui ponctuent un long travail de convention, jamais complètement clos[4].

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.

[4]. J'insiste sur ce point pour atténuer l'impression de stabilité que peut provoquer ce type d'enquêtes par entretiens.

Références

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), p. 169-208.

Chateauraynaud, F. & Trabal, P. 2003. *Internet à l'épreuve de la critique. Rumeurs, alertes et controverses au cœur des nouvelles technologies*. Rapport de Recherche, Paris, CNRS - Programme "Société de l'information".

Clot, Y. 1998. *Le travail sans l'homme ? Pour une psychologie des milieux de travail et de vie*. Paris, La Découverte/Poche.

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

Daniellou, F., Laville, A. & Teiger, C. 1983. Fiction et réalité dans le travail ouvrier, *Les Cahiers Français* (209), p. 39-45.

Dodier, N. 1995. *Les hommes et les machines. La conscience collective dans les sociétés technicisées*. Paris, Métailié.

Dodier, N. 1996. Ce que provoquent les infractions. Étude sur le statut pragmatique des règles de sécurité. In: Girin, J. et Grosjean, M. (dir.), *La transgression des règles au travail*. Paris, L'Harmattan, p. 11-37.

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

Joseph, I. 2004. *Météor. Les métamorphoses du métro*. Paris, Economica.

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

Orlikowski, W.J., Yates, J., Okamura, K. & Fujimoto, M. 1995. Shaping Electronic Communication: The Metastructuring of Technology in the Context of Use, *Organization Science* 6 (4), p. 423-444.

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.

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

de Terssac, G. 1992. *Autonomie dans le travail*. Paris, PUF.

Thévenot, L. 1990. L'action qui convient. In: Pharo, P., Louis (dir.), *Les formes de l'action. Sémantique et sociologie*. Paris, Éditions de l'EHESS, p. 39-69.

Weick, K.E. 2001. *Making Sense of the Organization*. Oxford, Blackwell.