L'institution de la sécurité ou comment s'en désintéresser

Dominique Boullier
Pascal Jollivet – Frédéric Audren

Quel discours de responsable portant sur les systèmes d'information pourrait éviter de conclure par un vœu, des recommandations, voire des prophéties en matière de sécurité ? Tout le monde en convient : l'extension infinie des capacités et des usages des réseaux n'a pas été accompagnée de la vigilance que l'on pourrait trouver dans n'importe quel ouvrage d'art ou réseau électrique. Est-ce à dire que les ingénieurs ne savent pas y faire ? Pas du tout, leurs recommandations et les outils logiciels qu'ils ont développés existent et permettraient sans aucun doute de réduire considérablement la portée des enjeux de la sécurité informatique. Mais le réseau n'en fait qu'à sa tête et des pratiques totalement imprévues n'en finissent pas de se développer d'une part et plus grave encore, les usagers ordinaires, ceux qui sont les plus susceptibles de revendiquer la sécurité pour leurs échanges de documents, pour leurs données personnelles, pour le commerce électronique, etc., ces usagers-là ne semblent vouloir qu'une chose, qu'on les laisse en paix avec ces problèmes, qu'on leur en parle le moins possible et que cela ne les oblige en rien à changer leurs habitudes. Or, la sécurité informatique a beau disposer de logiciels et d'architectures performantes, elle ne peut se passer de l'action au quotidien de chacun des utilisateurs pour faire tenir la chaîne de sécurité. Dès lors, comment expliquer qu'un supposé « besoin », identifiable dans tous les questionnaires et autres études marketing, ne parvient à se traduire dans les actes ? La « spécification des besoins » a-t-elle encore un sens quand les technologies sont déjà là et que le problème essentiel est de comprendre pourquoi si peu

LCN, volume 4, n° 3-4/2003, pages 219 à 238

de clients sont intéressés par un produit donné ? Nous ne parlons jamais de « besoins » précisément pour cette raison : il n'y a pas de « besoin de sécurité », la notion de besoin elle-même n'a aucun sens, pas plus lorsqu'elle est déclinée de façon plus détaillée en termes de signature électronique, par exemple. Les produits de la sécurité sur les réseaux existent bel et bien, les PKI sont proposées en offre commerciale et sont déclarées techniquement fiables et pourtant elles ne sont pas utilisées. Les pistes d'amorçage de la demande sont toujours aussi peu convaincantes, malgré les annonces.

Notre travail de chercheurs en sciences humaines n'est donc pas seulement un travail de spécification d'un nouveau type de PKI, en fait de certificats d'attributs, pour rendre service aux ingénieurs et aux développeurs : il consiste à refaire l'ingénierie de la demande de sécurité pour comprendre comment un produit, voire un concept, *a priori* indiscutable, peut se trouver dans l'impasse commerciale et pratique. Il est donc nécessaire de reposer autrement la question de la sécurité pour comprendre ce qui fait sens pour les acteurs dans leurs pratiques quotidiennes et en même temps de préciser toutes les qualités des éléments constituant cette chaîne de sécurité qui lui permettrait de tenir et surtout d'accrocher des utilisateurs.

Notre étude[1] (Audren *et al.*, 2002), nécessairement complexe à mener sur un tel sujet, dans une telle situation de « coulage » passif de l'innovation, et inévitablement incomplète, doit permettre de mieux comprendre ce qui se joue dans ces questions de sécurité dans les échanges informatisés. Mieux comprendre et donc prendre le parti de considérer[2] que les comportements des agents que nous observons sont rationnels, en ce sens qu'ils ont leurs raisons d'être, que chacun peut justifier des bonnes raisons qui le conduisent à ne pas appliquer les règles de sécurité que par ailleurs il pourrait appeler de ses vœux. Cette étude, conduite en liaison étroite avec des informaticiens, doit permettre de sortir les sciences humaines de leur rôle de voiture-balai du développement technique (ramasser les dégâts, en français plus académique, « évaluer les effets »). Mais elle doit aussi permettre de sortir les ingénieurs et les chercheurs des STIC de leur supposée maîtrise technique, pour voir à quel point ils manipulent des enjeux anthropologiques lourds, qui méritent souvent beaucoup plus d'attention que la discussion entre des solutions logicielles différentes. Pourtant, c'est au cœur de ces débats sur des solutions techniques que doit s'intégrer l'apport

1. Voir la note méthodologique présentant cette étude en annexe.

2. Comme le fait toute science humaine à visée à la fois compréhensive (et non analytique), située et non modélisante *a priori*.

des sciences humaines, car les stratégies de déploiement ne se construisent pas indépendamment des modèles et des architectures qui ont été décidées entre développeurs : c'est donc la conception même et le cercle de ses participants qui doivent être revus pour monter un système de « sécurité suffisante » où chacun des acteurs se voit reconnaître un rôle indispensable, qu'ils soient humain, logiciel, terminal ou règle administrative...

Composer une chaîne de sécurité

La diversité des médiations qui concourent à la sécurité sont trop souvent mentionnées pour mémoire, ce qui fait des systèmes informatiques, dont les IGC/IGP (infrastructures de gestion de clés publiques) des OVNI qui seraient développés « hors sol ». Or, de la qualité de leurs liens avec toutes ces médiations dépend toute la qualité de la chaîne de sécurité elle-même.

Physique et numérique : une question de détails

Il serait tentant de modéliser toute la sécurité des entreprises et des systèmes d'information, voire de réduire la sécurité à celle des systèmes d'information. Plus fréquemment encore, il est tentant de ne se préoccuper que de ce qui présente un intérêt pour un développeur, la sécurité des réseaux informatiques. Or, c'est la représentation même du système d'information comme « informatique » qui finit par intoxiquer le développeur : il n'existe pas de système d'information qui n'ait, à un moment ou à un autre, des réalités « physiques », hors des machines et des interfaces elles-mêmes, déjà bien matérielles. Le travail de conversion d'un monde dans l'autre (du virtuel au tangible) ne se fait jamais à un début de la chaîne pour être réversible à la fin : tout système d'information est un enchevêtrement de logiciel et de matériel mais aussi de technique et d'organisationnel. A chaque moment des activités de chaque agent, des conversions multiples s'opèrent du physique au virtuel, du matériel au logiciel, dans les deux sens. Le mot de passe est le cas typique du maillon faible supposé donner de la confiance alors qu'il est souvent reproduit sur des supports papiers du genre *post-it* ou communiqué oralement à un collègue sans autre précaution. Et ces comportements se justifient, ils ont du sens, mais ils ne sont pas pris en compte dans la chaîne de sécurité ou sont considérés comme déviants alors qu'ils sont pourtant le fonctionnement ordinaire le plus aisément observable. Les clés posent le même problème. Matérielles ou virtuelles, avec badge, code, ou autre, dès lors qu'il faut permettre d'accéder aux locaux dans lesquels sont les machines et/ou les données à protéger, on sort de la stricte modélisation informatique, on crée

nécessairement des conversions, des sources de manipulations, d'échange, etc., qui sont autant de maillons faibles dans la chaîne de sécurité. On peut alors mobiliser des signes *confidentiels* mis en évidence, des coffres ou encore des serviettes personnelles qu'on garde toujours avec soi : mais qui alors peut réellement prendre en compte tous ces maillons ? Cette question des contrôles d'accès, numériques ou physiques, constitue un point commun incontournable qui finit d'ailleurs parfois par résumer toute la politique de sécurité.

Des espaces, des réseaux, des contenus, des personnes

La sécurité doit dès lors s'appliquer à toutes les entités qui composent l'organisation en prenant en compte toutes les matérialités sous lesquelles elles apparaissent (et non seulement leurs représentants logiques au sein du système d'information). Les espaces sont fait de murs, de portes, de fenêtres, et sont sécurisés par des alarmes, des clés, etc. Les réseaux sont faits de fils, d'ondes, d'algorithmes, de serveurs, de flux, etc., et sont sécurisés par des mots de passe, des algorithmes de brouillage divers, mais aussi des clés d'accès à des machines. Les contenus sont faits de langage, d'images, de chiffres, de titres et de paramètres d'indexation, de documents convertis en bits et sont sécurisés par des empreintes, des chiffrements, des signatures ou des *login*/mots de passe. Les personnes sont faites de chair, de modalités sensorielles, d'identités institutionnellement reconnues, d'intentions et sont sécurisées par des empreintes, des documents d'identité, des barrières physiques, des surveillances et des historiques de leurs comportements. Ces personnes peuvent être catégorisées selon leurs fonctions ou selon des projets, ce qui change tout dans l'organisation de la sécurité.

Si une seule de ces entités, et une seule des matérialités sous lesquelles elles apparaissent sont oubliées, négligées ou si l'on se contente de leur supposer des intentions ou de leur prescrire des normes de comportement, la chaîne de sécurité est fragilisée. Il serait donc de première nécessité de penser une ontologie étendue, distribuée et plurielle dans ses formats, pour pouvoir prétendre traiter de la sécurité. Cependant le modélisateur fou qui se lancerait dans cette tâche y passerait sa vie et serait notamment incapable de traiter le changement et l'incertitude qui caractérisent les organisations.

Un dedans et un dehors : ennemis externes et ennemis intimes

Une politique de sécurité devrait décliner clairement les ennemis qu'elle se propose de traquer ou d'empêcher. La chose est assez aisée lorsqu'il s'agit d'imaginer des attaques de l'extérieur qui justifient tous les pare-feu les plus

sévères, d'autant plus que toutes les institutions, voire les particuliers, ont eu à subir ce genre d'attaques. Bref, chacun sait qu'il existe des êtres malveillants sur les réseaux. On n'en voit souvent que la trace sous forme de virus mais elle est suffisamment pénible pour faire accepter des mesures. Des mesures que l'on oublie vite, comme la mise à jour de l'antivirus par exemple. Mais tout cela n'est guère sournois et relève quasiment de la politique médiévale du château fort.

La menace moderne porte, elle, sur la propriété des informations, ou sur la vie privée. Et la sécurité doit bien sûr offrir des garanties dans ce domaine. Mais on touche alors à des ennemis intimes, à ceux qui peuvent être concurrents et parfois proches, pour être intéressés à l'exploitation de ces informations. A ce moment, plus de limites : tout le monde est suspect et le système de sécurité doit se tourner en système d'auto-surveillance des comportements des propres membres de l'institution. Mieux même, nous déclarent les personnes observées, c'est l'ingénieur système, l'administrateur, qui pourrait faire figure de suspect n° 1 car il possède les accès à toutes les données les plus personnelles, pour des raisons techniques. Certes, la déontologie que chacun lui suppose permet d'éviter une paranoïa interne fort déstabilisante... « mais quand même », on ne sait jamais vraiment ce dont il est capable et ce qu'il fait de ces accès, puisque personne ne contrôle le contrôleur, enjeu essentiel de toute politique, de sécurité comme d'autres domaines !

La population cible : les élus (informaticiens) génèrent des clones

Dans la constitution même des différentes populations ciblées pour les services de sécurité, c'est un véritable formatage de la population d'utilisateurs qui doit être assumé. Ce formatage dit bien que ce sont les utilisateurs qui vont se transformer pour s'adapter à la technologie offerte.

Le premier aspect de la notion de « formatage des usagers » porte sur la prise en compte de la formation et de toutes les médiations d'assistance que sont les documentations en ligne ou papier, les aides diverses, tout ce qui permet à un utilisateur de ne pas fuir une application donnée. Les usagers, contrairement à de nombreux lieux communs, sont prêts à faire des efforts remarquables pour s'adapter à des façons de faire à condition qu'on leur donne les moyens de faire cet investissement une bonne fois pour toutes et non dans l'incertitude, dans le provisoire, dans le non fiable (Boullier, 2001).

Le deuxième volet du formatage de la population porte sur les frontières mêmes du groupe ainsi défini par le système de sécurité offert. Dans tous les cas, certains seront dans un premier cercle et d'autres seront exclus, à la fois

à travers les types de services offerts et à travers le cycle de déploiement. Du point de vue du déploiement, la pratique communément répandue consistant à prendre en premier lieu, comme population cible, des *informaticiens*, risque d'avoir des conséquences normalisatrices et standardisatrices peu propices à l'adoption et à l'appropriation du système par les utilisateurs *lambda* ultérieurs. En effet, on ne peut guère apprendre à partir de ces cas. L'identification des *attributs* des différentes populations permettrait un ajustement plus fin par la médiation de la formation et de la sensibilisation méthodique de tous les utilisateurs.

On gagnera à effectuer une description systématique des propriétés ou des attributs de ces populations en cours de développement et avant toute mise en place, car les choix faits implicitement finissent par se durcir dans des choix d'architecture qui seront difficilement remis en cause. Lorsqu'on définit les attributs de ces populations cibles on s'oblige en effet à mettre à plat des frontières internes rarement discutées, des hiérarchies et des rôles implicites parfois et des principes de gouvernement de l'organisation ou du réseau qui doivent pouvoir être défendus sur le fond pour être déployés dans les cas particuliers.

A la recherche du garant perdu : le corps et l'Etat

La quête du garant est un élément constitutif de toute politique de sécurité (qui définit une ou plusieurs « autorités », un garant humain parmi les humains mais hors des humains quand même. On ne saurait la traiter à la légère car elle est au fondement même de l'institution et de la croyance qui les fait tenir toutes (Legendre, 1983). C'est pourquoi toutes les politiques de sécurité doivent fournir une réponse fiable pour enrayer la suspicion sur les médiations techniques et sur les personnes. Les systèmes d'information ne peuvent jamais prétendre assurer leur sécurité en se fondant sur eux-mêmes, ils doivent toujours renvoyer à un au-delà d'eux-mêmes où les manipulations informatiques ne semblent plus possibles. Les deux butoirs, au-delà du système d'information, souvent énoncés par les personnes que nous avons rencontrées qui reconnaissent toute la nécessité d'aller chercher ailleurs ce garant, sont :

– le corps comme on le voit dans le culte contemporain de la biométrie mais aussi dans l'importance des reconnaissances visuelles des personnes ;

– l'Etat comme origine supposée de toutes les autorités.

Nous avons ainsi deux extrêmes de la croyance moderne : l'individu que l'on pourrait réduire à ses propriétés biologiques, comme nous le propose la

science, et l'Etat, qui n'est pas engendré et qui est au-dessus des parties et des groupes, comme le propose le cadre politique de l'Etat-nation associé au modernisme. C'est au fond une tentative classique pour sortir ces questions de toute controverse politique en revenant à des identités indiscutables. Car le numérique a profondément perturbé ce régime des identités puisqu'on peut manipuler toutes ces entités à volonté.

La biométrie d'un côté pousse à un couplage toujours plus fort des techniques avec l'unicité du corps individuel, en feignant d'ignorer, comme tant de films de science-fiction l'ont pourtant prédit (cf. *Bienvenue à Gattaca* par exemple) que l'on pourra aussi simuler des organismes vivants comportant ces propriétés supposées non reproductibles. De façon intéressante, la technique « artificielle » par définition va chercher son salut dans du supposé « naturel » pour retrouver une confiance qui est, nous le verrons, strictement de l'ordre des conventions sociales.

L'Etat, à l'autre extrême, constitue un recours ultime face aux autorités autoproclamées en matière de sécurité. Le « tiers de confiance », dont la fonction est décisive dans les PKI, existe bien sur le marché, mais précisément parce qu'il n'existe que sur le marché, il est d'emblée suspect d'intéressement, il est pris dans des concurrences, qui sapent réciproquement leur légitimité. Toute recherche de garant doit buter sur un point ultime incontestable. Dans nos sociétés contemporaines, seuls les Etats assurent cette fonction mythique. Ce qui pose un problème de débordement constant dans une société en réseaux où tous les phénomènes à réguler ne se limitent plus à un territoire national. La sécurité et sa difficile mise en route dans les usages révèlent ainsi à quel point les cadres traditionnels de légitimité, ces garants ultimes, sont désormais inadaptés à une société globalisée. Et ce ne sont pas de simples organismes techniques de normalisation qui peuvent régler ces questions de confiance car il s'agit bien de partager du mythe, de supposer une entité qui serait elle-même indépendante des Etats, devenus de simples parties. Cette quête du garant ultime hors du social s'impose même aux communautés du logiciel libre. Pour se faire reconnaître par une communauté des développeurs, les membres participent à des rencontres physiques, des *key-signing parties* où chacun peut identifier les autres *de visu* (rôle du corps unique) d'une part et y associer une identité officielle, celle fournie par les papiers d'identité délivrés par les Etats d'autre part ! En circulant en lignes qui se font face et qui se présentent leurs papiers, les communautés du libre bouclent la boucle des garanties sur le corps et sur l'Etat, et disent ainsi clairement qu'aucune garantie ne peut être produite numériquement.

On comprend dès lors pourquoi les sociétés de service qui fournissent des solutions de sécurité font tout pour ne pas avoir à assumer la fonction de tiers de confiance, comme notre étude nous l'a montré : c'est d'un autre registre qu'il s'agit, registre symbolique dirait-on en anthropologie, qui assigne des places à chacun à la fois au sein d'un cosmos et dans une tradition (transmission et héritage sont des conditions de la garantie et de la croyance). Lorsque les débats portent sur les autorités, au sens quasi technique du terme (autorités de certification) ou au sens quasi disciplinaire internes aux institutions (qui a autorité pour autoriser ?), c'est toute cette chaîne de délégation de confiance et de croyance qui se mobilise, car aucune autorité ne peut s'auto désigner, contrairement à ce que pourrait laisser croire une vision toute puissante de la technique. On entre alors dans des justifications, dans des débats socio-politiques, dans la définition collective de ce qui peut fonder un accord, toutes choses qui supposent une autre « ingénierie », tout au moins un autre savoir-faire.

Mais cette question se retrouve au niveau du fonctionnement ordinaire à travers les enjeux de la signature électronique. Gérer la correspondance entre une fonction, une position dans l'organigramme, une personne à identité sociale connue et sa signature, ne représenterait aucun problème technique ou symbolique si tout correspondait de façon univoque. Or, ces dimensions peuvent se croiser de façon multiple en qualité et en quantité : plusieurs fonctions pour la même personne, une seule fonction pour plusieurs, des signatures en délégation, des fonctions identiques mais des positions hiérarchiques différentes ou même variables selon les projets, des signatures différentes selon les statuts, les documents, les projets... A chaque fois, ce sont donc des « attributs » différents qu'il faut manipuler de façon cohérente mais aussi de façon très concrète, très matérielle, dans des situations extrêmement diverses. A chaque fois, se pose la question de repérer au nom de quel principe doivent être mis en relation une signature et une des dimensions de l'entité en question, et dès ce moment, toute la chaîne d'autorité est sollicitée et questionnée, au-delà de toute modélisation logique ou mathématique qui cherche pourtant à produire une représentation totale du monde ainsi créé.

L'introuvable demande de sécurité

Toutes ces conditions techniques, matérielles et institutionnelles paraissent déjà si lourdes à mettre sur pied, qu'on suppose une grande demande pour se lancer dans un tel montage. Or, il n'en est rien.

La question est simple : « La sécurité dans votre école, qu'en pensez-vous ? » A question simple, réponses provocantes : « Moins je m'occupe de sécurité et mieux je me porte », « Je suis bien embêté pour réagir puisque, en fait, je n'ai jamais ressenti un besoin criant de sécurité ».

Voilà une situation qui contraste singulièrement avec le sens commun qui voudrait que le besoin de sécurité se fasse sentir plus fortement chaque jour. Telle qu'elle est organisée, la sécurité convient. Elle est *suffisante*. Par quel miracle nos enquêtés se trouvent-ils, à ce point, désintéressés des questions de sécurité ?

Examinons les propriétés de cette non-demande de sécurité, car les conséquences pour la construction du marché ne sont pas négligeables.

Le niveau de sécurité est toujours suffisant

C'est une observation récurrente pour les professionnels de la sécurité, comme les pompiers (Boullier et Chevrier, 2000) : on ne s'en occupe toujours que trop tard. Les situations ordinaires font oublier très vite les enseignements des périodes de crise ou les prévisions des professionnels. Plus encore, la sécurité doit toujours être invisible et non pénalisante pour l'usager, ce qui conduit à admettre tous les niveaux de sécurité dès lors qu'on en a pris l'habitude. Pas de critère objectif sur ce plan, tout est question d'habitude. Ainsi, aucune des personnes interrogées n'a formulé explicitement une échelle du tolérable et de l'intolérable en matière de sécurité. Aucune ne nous a signalé qu'elle considérait telle mesure ou telle mesure comme une attaque contre le raisonnable. Nos enquêtés produisent un discours très offensif sur leur indépendance, leur liberté mais, personne n'a jamais avancé l'exemple d'une mesure de sécurité considérée comme attentatoire aux principes défendus par exemple dans l'université. Même les plus critiques s'adaptent et finalement « font avec ». L'essentiel est en fait d'organiser le retour au calme, le « retour au naturel » des situations car rien n'est plus lourd sur le plan cognitif que de devoir en permanence remettre en cause ses routines.

Cette satisfaction par défaut (on est satisfait si on n'en entend plus parler) pose un vrai problème au marketing des solutions de sécurité pour créer cette demande, pour la rendre explicite. Elle ne doit pas être interprétée comme une résistance ou une posture critique vis-à-vis du sécuritaire en général. Mais par expérience dans ce domaine, chacun sait que « le mieux est l'ennemi du bien », car des mesures trop lourdes et une mobilisation constante pour réviser les routines (car c'est ce que suppose une vraie politique de sécurité) finissent par générer tant de perturbations que chacun

tente d'y échapper. Un projet de développement d'IGC ne peut espérer se soustraire à cet impératif de création de la demande car la sécurité se fait avec les agents ou ne se fait pas, toutes les contraintes non justifiées ou seulement trop pénibles se trouvant très vite détournées. On peut à l'inverse mettre en valeur cette capacité des acteurs à accepter de nouvelles pratiques de sécurité, comme nous l'avons observé à l'occasion du plan Vigipirate que personne n'a vraiment contesté. C'est un atout qui doit être exploité et que les professionnels de la sécurité connaissent bien puisque les catastrophes sont les seules occasions pour eux de faire passer de nouvelles règles et de nouveaux comportements. A condition qu'ils se stabilisent pendant suffisamment de temps pour devenir des routines et se faire oublier.

La déviance est normale

Cet impératif de « sécurité suffisante » est d'autant plus justifié de la part des acteurs au sein des institutions que toute opération de ce type suppose en même temps la mise en place d'une surveillance des comportements de chacun. Toute politique de sécurité doit, pour être conséquente, aménager son régime de police. La question n'est plus « qui peut faire quoi ? » mais « qui a fait cela ? ». La sécurité suppose que l'on puisse imputer des responsabilités, des fautes et des erreurs. C'est là un aspect qui inquiète sérieusement les acteurs et ne contribue pas à motiver la demande de sécurité. Toute politique de sécurité pose des normes plus ou moins contraignantes à respecter : « il faut fermer sa porte à clé », « il faut porter son badge », « il faut signer les documents »... Mais qu'arrive-t-il lorsque le badge personnel est perdu ? Quid lorsqu'un vol a été commis parce que la porte n'était pas fermée ? Que se passe-t-il si l'argent engagé ne devait pas l'être sur ce poste ? Le besoin de sécurité est inconcevable sans une chaîne précise de responsabilité. Pour le dire brutalement, poser des règles de sécurité, c'est multiplier le risque de ces infractions à la sécurité... C'est là un balancement bien connu des juristes. Mais il devient proprement paralysant dans certaines situations, dans certains univers. Ce contrôle généralisé fait basculer dans une autre problématique : privé-public. Désirant rationaliser son service, un responsable a exigé de ses subordonnés qu'ils lui confient tous leurs codes d'accès sur leurs ordinateurs. Cette décision provoque un grand malaise dans le service. A-t-il accès à des informations privées et personnelles ? Peut-il contrôler à un temps T le travail réalisé ? etc.

Pour rendre la situation viable et tolérable, on imagine sans peine que les acteurs s'efforcent de ne pas mettre en cause systématiquement leurs collègues lorsqu'une règle a été manifestement violée. On tolère une certaine déviance. On en trouve une belle illustration dans la « zone protégée » d'une

école. Afin de limiter les nuisances sonores (la porte claque très violemment quand elle se ferme) ou encore pour ne pas s'encombrer de son badge lors d'une absence momentanée, quelques personnes bloquent la porte du sas avec un annuaire ou des magazines... La forteresse se transforme pour quelques minutes en laboratoire « portes ouvertes ». C'est là une violation élémentaire et flagrante des règles de sécurité qui fondent l'existence de cette « zone ». Pourtant, l'événement est accueilli au pire par des grognements, au mieux par des haussements d'épaules ou un sourire ironique. L'écart est toléré. Ce modèle ou ce sous-régime de « l'arrangement » (Boltanski et Thévenot, 1991) repose en fait sur une cosurveillance des déviances : « tu ne me signales pas pour mon laisser-aller, j'en fais de même pour toi. »

On bloque ainsi la remontée en justification des pratiques mais l'organisation s'installe alors dans une sorte de loi du silence qui fait le lit de tous les pouvoirs occultes. En tous cas, ce principe de l'arrangement, certes pratique et adapté à une sécurité qui convient, suffisante, va directement à l'encontre de « l'institution de la sécurité » et de sa possible discussion. L'arrangement s'explique aussi par le fait que toutes les prétentions institutionnelles en matière de sécurité sont toujours maximalistes et perçues comme abusives. On mesure alors que les plus beaux formalismes de sécurité obligent à rendre possible l'imputation de toutes les fautes (et leur sanction), les plus mineures même, dès lors que ces maillons faibles sont à la base même de la chaîne de sécurité. La responsabilité permanente de tous vis-à-vis de tous peut générer une atmosphère du soupçon que le fonctionnement traditionnel préfère éviter en se reposant d'autant plus sur les arrangements non formalisables.

Dans un tel contexte, on voit émerger un conflit entre :

– les tenants d'une formalisation accrue de tout le fonctionnement, puisque les comportements humains restent le point faible, quitte à générer des pratiques de contournements plus nombreuses encore ;

– et ceux qui perçoivent la nécessité d'une pratique de sécurité suffisante qui s'accommode aussi des déviances normales pour pouvoir être vraiment appliquée.

La demande de sécurité se construit dans ce conflit qui ne lui donne guère de chances de mobiliser les acteurs, alors qu'elle repose précisément sur cette mobilisation constante pour être efficace.

L'obscure grammaire de la sécurité et les paradoxes de la transparence

Tout formatage technique touchant d'aussi près une institution fait intervenir un vocabulaire, des entités, des catégories qui prennent des sens fort différents selon les acteurs. Les niveaux de sécurité, les procédures techniques de certification, les différentes autorités, etc., tels qu'ils sont décrits par les développeurs des systèmes de PKI ou même par les juristes spécialistes, n'ont aucune chance d'être appropriés par les utilisateurs *lambda*. Jouer pour ces raisons la carte de la transparence, qui éviterait à l'utilisateur de comprendre exactement ce qu'il fait grâce à des automatismes, peut s'avérer contre-productif, voire indéfendable en droit, et se réduire à un rituel de signature totalement délégué à l'application en question, avec les surprises à venir lorsque les garanties attendues sont totalement inadaptées.

Cette « transparence » est en fait ambivalente vis-à-vis de l'utilisateur dès lors que l'on a une approche globale d'ergonomie cognitive. Ainsi, une « transparence opératoire » peut se révéler, au niveau cognitif, totalement « opaque » pour l'utilisateur. Autrement dit, une tension contradictoire existe souvent entre la « transparence » d'un applicatif et la compréhension par l'utilisateur de « ce qui se passe ». Or, tout particulièrement pour la PKI, la compréhension par l'utilisateur de « ce qui se passe » quand il active telle ou telle fonction sécuritaire fait partie intégrante de l'efficacité du système de sécurisation.

L'exemple du message demandant à l'utilisateur « l'autorisation en lecture » de sa clé privée, lorsque qu'il active la fonction de déchiffrement, est assez représentatif de ce type de dilemme :

> « Donc là, quand j'ai installé le certificat sur mon poste de travail, j'ai demandé à être prévenu à chaque fois qu'une application accède à ma clé privée. C'est pourquoi on a cette boîte de dialogue qui apparaît, [une fenêtre qui lui demande s'il est d'accord pour autoriser l'accès par un logiciel, en lecture, à sa clé] et dans ce cas-là, je peux envoyer. » *(Responsable d'exploitation)*

Ici, on *rallonge* donc la chaîne des opérations que l'utilisateur doit réaliser afin de mettre en œuvre cette fonction sécuritaire, diminuant en cela l'ergonomie *opérationnelle* du dispositif. Mais en même temps on *augmente* le niveau de sécurité procurée à l'utilisateur (il est certain que personne ne va pouvoir lire à son insu sa clé privée) grâce à une *meilleure ergonomie cognitive* (il comprend et maîtrise davantage ce qui se passe). Le directeur du département informatique d'une grande entreprise étudiée explique d'ailleurs que, pour l'instant, il hésite entre trois configurations proposées à l'utilisateur :

– l'absence totale de confirmation de la lecture de la clé par le logiciel (ce qui correspond à une « transparence » totale pour l'utilisateur) ;

– une demande de confirmation d'accès, validée uniquement par un *clic*, *via* une fenêtre qui s'ouvre ;

– une demande de confirmation d'accès validée par un *mot de passe*, correspondant à un PIN (pour une carte à puce notamment).

Le directeur technique de la société de service a, lui, une position très tranchée :

> « Si... j'ouvre le lecteur, et puis derrière, je peux "signer" un certain nombre de documents, là il y a un problème majeur. [...] Il y a des lecteurs qui fonctionnent comme ça... Je m'identifie auprès du lecteur, et puis derrière, j'envoie les mails que je veux. Ça veut dire que c'est automatisable. Ça veut dire qu'il n'y a pas eu d'action physique de signature. Donc il n'y a pas de valeur. Si derrière il n'y a pas d'approbation, il n'y a pas de valeur. »

On voit donc bien ici – sans même mentionner les dimensions juridiques – que la « vertu de transparence » peut se révéler, en matière de sécurité, *contre-productive*.

La question de la « transparence » de la PKI n'est donc pas si univoque : elle participe d'un compromis qui touche au cœur même de la performance sécuritaire du système.

Contrairement à la sécurité physique, la sécurité numérique est en effet difficilement « palpable », appréhensible de façon directe par l'utilisateur standard. La grammaire de la sécurité électronique est effectivement complexe, pour un non-spécialiste, ne serait-ce que sur un point qui constitue pourtant le fondement même d'une IGC, la double clé asymétrique : comment comprendre, quand on n'est pas un spécialiste ou quand on n'a pas l'occasion de sérieusement se former, que la sécurité procurée par l'IGC provient d'une clé qui est « publique », disponible pour tous, bien qu'elle soit complémentaire d'une autre clé « privée » et secrète ? Comment comprendre que cette complémentarité entre les deux clés soit traçable dans un sens (clé privée-clé publique) mais pas dans l'autre, et que tout cela repose sur un défi mathématique non résolu de factorisation de longs nombres premiers ? Et si l'on ne comprend pas ces fondements conceptuels et théoriques, comment faire confiance à un système non appréhensible par les sens ? Et s'il n'y a pas de compréhension, il n'y aura pas de confiance envers le dispositif, et il n'y aura pas d'appropriation et d'usages qui se développeront.

Or, les utilisateurs possèdent des catégories ordinaires pour penser leurs questions de sécurité qui peuvent être utiles à exploiter pour simplifier un

cadre cohérent de compréhension de ce qu'ils font. La dimension sociale notamment en est un élément : la confiance et la réputation se construisent à travers des pratiques sociales et peuvent servir de repères pour valider des opérations dans un monde inconnu ou innovant. Il s'agirait donc ici de se placer non plus du point de vue de l'excellence technique qui a empilé les fonctionnalités et les cas de figure à partir de ses propres ontologies, ni du point de vue de l'excellence juridique qui prétendrait tout verrouiller par avance et s'enraciner dans des ontologies à longue histoire produites par le droit. C'est en se plaçant du point de vue de l'utilisateur et des enjeux institutionnels éprouvés ou expérimentés par les sujets que l'on peut redéfinir ce qui est enjeu essentiel ou non. Le sens de l'intérieur et de l'extérieur, des autorités, des menaces, sont ainsi à prendre en compte dans la mise en forme des ontologies pour mettre à disposition une grammaire de la sécurité qui soit enfin appropriable.

Les applicatifs comme moteurs de diffusion : transparence et compréhension ne marchent pas ensemble

Rappelons l'évidence : personne « n'utilise un ordinateur pour produire de la sécurité », personne « n'utilise des logiciels de PKI ». Ce découpage fonctionnel n'a pas de sens du point de vue de l'activité d'un utilisateur, au sens où l'ergonomie cognitive la définit (par distinction avec la tâche). Ce sont avant tout ses objectifs de production et d'échange d'information, de valeur variable, dans des réseaux variables qui ont un sens. C'est d'ailleurs tout le problème d'une politique de sécurité de prétendre être généraliste alors qu'elle doit être spécifique et adaptée à certains types de réseaux, certains types d'échanges et certains types d'informations, et variables dans tous ces cas.

C'est pourquoi les `applicatifs` se sont révélés comme les véritables moteurs d'une PKI, qui n'apparaît plus aux yeux de l'utilisateur que sous-jacente, voire « invisible », à la rigueur sous la forme d'un bouton. D'ores et déjà au niveau même de l'ergonomie, des indicateurs de niveaux de sécurité visuels peuvent être intégrés et directement accessibles pour l'utilisateur, au-delà de l'alternative entre le bouton qui rend tout « transparent », c'est-à-dire impossible à contrôler et à comprendre, et le tableau de paramétrage qui demande une expertise rare. Ainsi, lorsque l'un des logiciels offre des barres de visualisation d'un niveau de sécurité, on offre un accès rapide à une représentation graphique mais cohérente d'un ensemble d'informations complexes.

La visualisation devrait offrir deux aspects : les niveaux de sécurité redéfinis par une ontologie qui agrège certaines propriétés d'une part et les

niveaux de fiabilité des « recommandataires » ou autorités qui ont enregistré ces signatures (par exemple) d'autre part, pour reprendre cette propriété offerte dans la communauté du libre. Ce point est important pour visualiser la chaîne de délégation de la confiance ainsi produite, car il ne s'agit jamais que de délégation, sans source ultime convoquée à chaque instant. Il est plus opérationnel de rendre visibles ces médiations techniques ou humaines qui permettent de certifier les différents maillons que d'attendre une hypothétique garantie ultime.

Comment faire exister un non-marché ?

Les quelques pratiques observées, les quelques retours d'expériences constitués, s'ancrent toujours dans des réalisations de sécurité relatives, bien loin des normes « certifiées ».

On réalise combien on est loin des affirmations qui présentaient jusqu'à peu l'IGC comme « la » solution définitive et absolue aux problèmes de sécurité et de confiance sur les réseaux électroniques. Ces slogans relèvent soit d'un technicisme déterministe (le modèle technico-conceptuel de l'IGC engendre une sécurité incassable) soit de la réclame de foire (l'IGC : la solution pour votre sécurité).

Le problème des modalités de vente de la sécurité apparaît de façon criante lorsqu'il est question de proposer aux clients un dispositif assurant un niveau de sécurité plus élevé, dans lequel le client-utilisateur serait lui-même identifié par des dispositifs de signatures et certificats fondés sur une IGC.

> « L'autre problème des banques, c'est comment facturer ça à nos clients.
>
> Pourtant, certaines banques facturent les services supplémentaires sur internet...
>
> Oui, mais elle le facture *à un certain niveau*, avec login-mot de passe. Alors qu'est-ce qu'elles font ? Elles augmentent leurs tarifs permettant qu'il y ait plus de sécurité ? Mais là, comment elle vous le vend ? Elle vous explique que c'était pas sécurisé avant ? » (Société de services)

Le problème de la vente de cette sécurité nécessairement relative se retrouve avec la même acuité en intra-organisationnel. L'expérience de l'organisation utilisatrice que nous avons étudiée est ici tout à fait éclairante. Ayant développé une IGC à usage interne, elle n'est pas soumise à l'impératif d'une signature qualifiée. Elle a fait le choix, soutenable, de s'en affranchir et de ne viser qu'à une *amélioration* du niveau de sécurité, ne permettant pas aux certificats d'avoir une valeur légale.

La difficulté émerge alors quand il s'agit de « vendre » aux utilisateurs finaux les services issus de cette infrastructure, notamment les services de signature non qualifiée.

Un rapide bilan est plutôt inquiétant pour les stratégies de vente :

– Des clients utilisateurs de banque à domicile à qui l'on « vend » une première génération de téléservices en leur vantant la sécurisation élevée des transactions qu'elle permet, à qui l'on prévoit de proposer ensuite une deuxième génération qui nécessite d'expliquer que la première n'était pas si sécurisée que ça...

– Des utilisateurs-prospects d'une organisation dite *à risque* à qui l'on propose un dispositif de signature en promouvant la sécurité des communications qu'elle autorise, à qui l'on prévoit de dire sous peu que ce n'était pas une vraie signature... ce qui est la raison pour laquelle on va leur en proposer une autre !

Vu sous cet angle, comment s'étonner que le marché ait du mal à « prendre » et que les déploiements dans les organisations soient si difficiles ? Comment s'étonner qu'un vendeur de produits et services en sécurité électronique ait du mal à convaincre son prospect de passer à l'acte d'achat ? De la difficulté d'un responsable informatique ou d'un responsable de la sécurité à argumenter auprès de sa direction générale la pertinence de cet investissement sécuritaire ? Ou de la difficulté d'un chef de projet interne à « trouver » des utilisateurs-prospects volontaires pour cette aventure ?

La construction de la demande dont on trouve trace dans un argumentaire de vente supposé bute aussi sur *l'absence d'objectivité du risque*, par définition non advenu et toujours impossible à garantir totalement.

Ce dilemme de l'économie du risque peut trouver une résolution partielle à travers des actions de révélation des risques, d'objectivation et d'évaluation du niveau de risque effectif attaché à une organisation donnée, particulière. Mais cette activité est coûteuse, et nombre d'organisations sont réticentes à dépenser pour un service d'audit qui ne pourrait que révéler des défaillances organisationnelles. Là aussi, sauf circonstances particulières dues par exemple à l'advenue récente d'un incident effectif, il s'avère ardu de « vendre » cette activité sécuritaire particulière qu'est la révélation de défaillances.

De plus, la solution logicielle proposée, comme nous l'avons vue, n'est qu'un élément d'une stratégie globale. La valeur effective de l'investissement matériel et logiciel envisagé pour la sécurité dépendra avant tout de l'activité que l'entreprise saura développer autour de ces biens et services, et de la culture et des pratiques sécuritaires particulières à son

organisation. La valeur du bien ou service en sécurité électronique dépend de façon cruciale de l'actif spécifique organisationnel de l'entité utilisatrice – la culture et les pratiques sécuritaires de l'organisation concernée.

Mais la valeur économique d'une signature, et des investissements en IGC qui la sous-tendent, est encore plus incertaine si elle ne peut prétendre au statut de valeur légale, qualifiée. La solution technique IGC est supposée « garantir » la sécurité des réseaux informatiques dans les organisations – du fait de la valeur des signatures, de la robustesse et l'inviolabilité de l'algorithme de double clé asymétrique fondé sur les nombres premiers. Or, nous dit l'un des responsables d'implémentation d'une IGC : « Avec la signature électronique, *a priori*, les ingénieurs-techniciens informaticiens disent : *non, ça ce ne sera plus possible de la contester* ! On ne contestera pas l'algorithme [PKI], probablement, c'est à peu près sûr. [Mais] on *contestera les conditions d'emploi.* »

On peut ainsi identifier trois types de critères qui contribuent à constituer la valeur économique d'un dispositif de signature :

– l'engagement de *moyens* (techniques, organisationnels et institutionnels) par l'opérateur de sécurité, visant à étayer la robustesse, relative, du dispositif sécuritaire mis en œuvre, et des signatures qui en sont issues ;

– l'engagement de *responsabilité* à travers notamment des garanties financières, par niveau, selon des prix et des types d'utilisations préétablis de différents types de signatures ;

– la *confiance* que l'on porte à cette institution, qui est une appréciation subjective de l'assurance que ce qui est annoncé par l'institution soit effectivement réalisé, que ces engagements soient crédibles.

Cette triple incertitude de la valeur de la signature – dépendant toujours du degré de confiance que l'on porte à l'opérateur sur ces engagements, de « l'attente » de la mise à l'épreuve par l'incident et la preuve, et du relatif flou sur *qui* aura la charge de cette preuve et comment elle sera apportée – engendre un certain *attentisme* de la part des utilisateurs. Ainsi, le choix a été fait dans l'organisation citée, non seulement de ne pas prétendre à une valeur « légale » de leur signature, mais également de n'y attacher, dans un premier temps, aucune responsabilité.

Comment créer le marché d'un bien public ?

Le développement des activités économiques sur les réseaux électroniques de type internet, extranet ou intranet milite en faveur du rapide établissement d'outils « équivalents » à la signature « papier » dans le

monde numérique. Il existerait ainsi une demande au niveau macro-économique pour la signature numérique – en tant qu'elle favorise le développement d'activités économiques dans une société de la connaissance et des réseaux numériques – mais l'on ne parviendrait pas à faire émerger une offre durable à travers les mécanismes de marché.

En sciences économiques, un tel bien qui correspond à une demande globale mais qui ne trouve pas satisfaction à travers les mécanismes de marché d'offre et de demande à l'initiative d'acteurs privés, peut correspondre à ce que l'on dénomme un *bien public* ou *bien collectif*. Et si, à l'instar de la sécurité nationale et de la justice, la signature-authentification était un bien public, qui devait, au moins en partie, être pris en charge par l'Etat ? Ce qui correspondrait exactement à la quête de garant que nous avons déjà décrite chez tous les utilisateurs et qui finit par bloquer toute la dynamique commerciale. Ce serait prendre acte du fait que la signature électronique-IGC, avant d'être une technique informatique ou organisationnelle, est bien une *institution*. Ce serait par ailleurs reconnaître que le déclenchement d'un effet réseau est une condition pour que ces systèmes d'échange fonctionnent. En effet, la *valeur d'usage* d'une signature, à savoir l'utilité qu'un individu retire de son utilisation, est conditionnée par le fait que d'autres personnes l'utilisent également. C'est ce que les économistes nomment externalités positives de réseau, ou effets externes de réseau.

Rappelons-nous ici le témoignage du directeur prestataire de services en signature électronique qui dit en substance : « moi, ça ne me gênerait pas que l'Etat réalise le travail d'authentification d'un certificat numérique public. Mon métier étant des services sur la signature numérique ça constituerait plutôt un levier à mon activité économique. Car en l'état actuel des choses, on ne sait pas où est le marché des AC, personne ne sait financer cette activité. » Pour autant, le montage n'a rien de simple. Technologies, marchés, clients et institutions des PKI et des signatures électroniques sont non seulement des entités floues, en bonne partie indéterminées, mais elles entretiennent de plus entre elles des relations d'interdépendance. Ce sont des entités coévolutives.

Deux arguments principaux militent cependant en faveur d'un cadre législatif et institutionnel « souple », qui maintienne suffisamment de marges pour être apte à évoluer. Tout d'abord, la phase d'émergence industrielle dans laquelle se situent les technologies et marchés de la signature électronique exige de laisser un cadre suffisamment « lâche » pour que puisse se réaliser l'exploration de la variétés techno-économique de différents « montages ». On ne saurait complètement réglementer une activité dont on ne connaît pas encore vraiment les contours. Le deuxième

argument tient à une spécificité de ces biens et services de « sécurité » électronique : la sécurité, réelle, ne peut être que relative et imparfaite. Une réglementation qui se donnerait comme référence une sécurité « absolue » ne pourrait être qu'inapplicable et risquerait d'inhiber le développement de l'activité plutôt que de le stimuler.

Ingénierie de *l'imperfection adaptée*, centrée sur les usages ordinaires, et « formatage » des utilisateurs à la grammaire quotidienne de la sécurité, semblent constituer deux maillons-clés, généralement négligés, du management de l'intégration d'une IGC et de la génération d'usages d'ampleur dans l'organisation.

Bibliographie

Audren F., Boullier D., Jollivet P., L'institution de la sécurité ou comment s'en désintéresser, rapport 1.1. RNRT, Icare (Infrastructure de confiance sur des réseaux Internet et mobiles), juillet 2002.

Boltanski L., Thevenot L., *De la justification. Les économies de la grandeur*, Paris : Gallimard (NRF), 1991, 485 p.

Boullier D., Chevrier S., « Grammaire de l'urgence : les sapeurs-pompiers, experts du risque », *Les Cahiers de la Sécurité intérieure*, n° 22, 4e trimestre 1995.

Boullier D., Certaines J.-D. (de), « L'art du compromis socio-technique dans l'innovation hospitalière : le cas des systèmes de communication et d'archivage d'images médicales (P.A.C.S.) », *Sciences sociales et Santé*, vol. X n° 3, 1992, p. 75-103.

Boullier D., Chevrier S., *Les sapeurs-pompiers : des soldats du feu aux techniciens du risque*, Paris : PUF, 2000.

Boullier D., « La vidéosurveillance à la RATP : un maillon controversé de la chaîne de production de sécurité », *Les Cahiers de la Sécurité intérieure*, n° 21, 3e trimestre 1995.

Boullier D., « Les conventions pour une appropriation durable des TIC. Utiliser un ordinateur et conduire une voiture », *Sociologie du Travail*, 3/2001, p. 369-387.

Boullier D., « Les études d'usages : entre normalisation et rhétorique », *Annales des Télécommunications*, 57, n° 3-4, 2002, p. 190-209.

Jollivet P., (avec Dieuaide P.), « TIC, Artéfacts et Redéploiement de la Norme de Consommation : Que peut nous apprendre le modèle "Hacker" ? », *Actes du colloque Conférence SASE 2003* (Society for the Advancement of Socio-Economics), Aix-en-Provence, 26-27-28 juin 2003.

Jollivet P., « Les NTIC et l'affirmation du travail coopératif réticulaire », in *Le Capitalisme Cognitif*, ouvrage collectif coordonné par Azaïs C., Corsani A. et Dieuaide P., L'Harmattan, 2001.

Legendre P., *L'empire de la vérité. Introduction aux espaces dogmatiques industriels*, Paris, Fayard, 1983.

Annexe

Méthodologie

Les observations que nous avons conduites ont été réalisées dans le cadre d'un projet RNRT I-Care (infrastructure de confiance sur des réseaux internet et mobiles), qui s'est déroulé de septembre 2001 à septembre 2003, avec les partenaires suivants : Thalès, ENST, Eurecom, Ecole des Mines d'Alès, T. Piette-Coudol avocat, CEA-LETI, Francert. Nous avons dû prendre en compte la difficulté d'accès à des entreprises ordinaires équipées en routine de systèmes de PKI. C'est donc une approche détournée qui décompose notre objet qui nous a permis de poser les spécifications socio-techniques de systèmes de sécurité basées sur des clés asymétriques publiques. Cette difficulté méthodologique était en elle-même symptomatique puisqu'elle confirmait le constat de départ : les techniques existent bien mais le marché n'en veut pas. La sécurité est un problème, certes, mais les usagers ne veulent pas s'y intéresser sérieusement. Nous avons donc effectué des observations sur des sites susceptibles d'être équipés, deux écoles d'ingénieurs, en cherchant à repérer les enjeux organisationnels qui sous-tendaient les pratiques actuelles et qui pouvaient orienter les spécifications futures, en termes de développement ou en termes de stratégies de déploiement. Les observations ont été réalisées à partir de 21 entretiens approfondis avec des personnels divers dans des fonctions enseignantes, techniques ou administratives.

Obtenir des retours d'expérience de la part d'utilisateurs réels des systèmes existant sur le marché présentait un défi plus important car, comme dans tout effet réseau, le premier utilisateur est toujours pénalisé et doit être volontariste dans la mesure où ses partenaires n'utilisent pas le même système. Nous avons donc adopté un recrutement de sites utilisateur très hétérogène en visant surtout la diversité des partenaires dans la durée (soit 2 fois 11 entretiens, à un an d'intervalle) :

– une grande entreprise en phase pilote, puis « réelle » (2 x 8 entretiens + observation) ;

– un réseau logiciel libre utilisateur courant (2 x 2 entretiens plus observation participante) ;

– une PME qui commercialise une solution de sécurité (2 x 1 entretien).

Dans ces trois cas, la demande de sécurité et son émergence sont radicalement différentes.