Serge Proulx

Professeur titulaire. École des médias. Université du Québec à Montréal.
Professeur associé. Télécom ParisTech.

La sécurité dans un monde numérique - Éditorial

E. Kessous et S. Proulx (2007)

Sécurité du monde numérique/Security in the digital society.

Présentation du numéro

La thématique de la sécurité devient centrale pour le développement de l'économie numérique, elle concerne principalement l'Internet pour lequel le développement du haut débit conduit à de nouveaux risques pour l'utilisateur (trojan, spams, phishing, ..), mais s'étend depuis à d'autres sphères de la société de l'information, elles aussi concernées par la numérisation : les téléphones mobiles, la voix sur IP et plus récemment les dispositifs d'identification ou de contrôle (carte RFID, biométrie…). Cette thématique fait souvent l'objet de regards experts mesurant l'innocuité des ondes électromagnétiques, la fiabilité des protocoles et du code informatique ou des méthodes d'authentification biométrique. Sans la délaisser totalement, les sociologues et les économistes investissent peu cette question. Pourtant la sécurité renvoie également à une dimension plus personnelle, mais également plus politique, portant sur le respect de la vie privée et la constitution d'une identité numérique.

L'une des raisons de cette désaffection sur ce sujet central tient à ce que « la sécurité » en tant que telle n'est pas une catégorie facile à manier en sciences sociales. On parle plus aisément de « sentiment de sécurité », de confiance, de « société de la surveillance » ou de risques. Autant de catégories qui permettent de circonscrire notre objet par des facettes d'analyse bien différentes. La sécurité dans l'Economie du numérique est souvent évoquée pour valoriser l'efficacité d'une technologie (comme l'open source) ou pour expliquer les freins psychologiques à l'émergence de nouveaux marchés (comme le commerce électronique dans les années 2000). Souvent exogène aux modèles économiques, la notion de confiance n'est pas mieux lotie. Combien de fois avons-nous entendu l'incantation ? Il faut « rétablir la confiance », élément manquant, mais au combien indispensable, lorsque tous les paramètres objectifs de sécurité sont réunis. La confiance est parfois considérée comme le seul choix possible – le choix rationnel – en situation de risque. De telle sorte que certains auteurs ont pu affirmer que l'on n'avait pas besoin de la notion et qu'il fallait la réserver aux relations intimes (Williamson, 1973).

Pourtant un des moyens d'établir la confiance est d'établir des règles, claires et reconnues organisant la transparence des marchés. Mais ces règles peuvent elles-mêmes faire l'objet de polémique – être l'objet d'une affaire pour reprendre les termes de Chateauraynaud et Thorny (1999) – aboutissant à une crise cumulative de confiance. En sociologie, la notion de confiance a fait l'objet d'une littérature abondante. On la trouve historiquement chez des auteurs comme Simmel, Weber ou Luhmann. La confiance est une entité sociale, un mode de coordination en soi, un des principes supérieurs commun des six cités repérés par les auteurs des *Economies de la grandeur* (Boltanski et Thevenot, 1991). Sans être toujours bien définie par les auteurs qui la mobilisent, la confiance sert de catégories d'analyse à des phénomènes très variés : histoire des sciences, marchés financiers, institutions politiques, monnaie, éducation, etc. Si on peut considérer qu'en économie la confiance n'est nulle part, en sociologie elle semble se dissimuler partout. Ce partage des rôles est symptomatique de la manière dont les deux sciences sociales perçoivent

l'étanchéité de leurs disciplines réciproques, sans aucune hybridation et mutualisation possible (Orléan, 2000).

La notion de risque semble avoir un destin mieux partagé dans les sciences sociales. Pourtant, encore une fois, les disciplines y mettent des contenus forts différents. Elément constitutif de la naissance de l'Etat providence et du droit social contre le droit civil (Ewald, 1989), la notion de risque permet d'intégrer dans les outils de l'économiste les différents états de nature envisageables. La théorie de l'utilité espérée a néanmoins un statut ambiguë car elle permet à la fois d'évaluer la perception par rapport au risque et le revenu marginal de l'agent. (Allais, 1953). Le risque en sociologie est, au contraire, un moyen de mesurer les comportements déviants à la norme (la « prise de risque ») tant aux niveaux individuel que collectif, notamment lorsqu'il s'agit d'évaluer les politiques publiques (Perreti-Watel).

Ce numéro des *Annales* a pour vocation d'aborder quelques-uns des aspects de cette dialectique du risque et de la sécurité, liée au développement des technologies numériques. Les différentes contributions abordent la question des technologies de manières assez différentes mais souvent complémentaires. Ainsi, dans sa contribution, Emmanuel Kessous, analyse la diffusion de nouvelles technologies numériques comme l'émergence d'un nouveau système expert (au sens de Giddens). L'usager perd ses repères, la concurrence entre les offres ainsi que l'incorporation d'un supplément d'informatique dans les réseaux font réapparaître la possibilité de pannes générales. éventualité que l'on pensait révolue. Ces « alertes » réduisent le niveau de confiance que les utilisateurs peuvent avoir dans les « représentants » des systèmes experts et souligne la nécessité de règles communes de régulation, notamment en ce qui concerne la *privacy* et les niveaux de responsabilité des diffuseurs de nouvelles technologies.

C'est une posture plus radicale, mais pas nécessairement contradictoire, qu'adopte Meryem Marzouki dans sa contribution. A partir d'un travail de recension des évolutions juridiques sur le plan français et européen, en ce qui concerne notamment les politiques de sécurité et de contrôle des identités, elle fait l'hypothèse d'une transformation de la société, passant d'une situation de « confiance mutuelle » à une situation de « suspicion généralisée ». Pour le montrer, l'auteur analyse les innovations des lois récentes en matière de sécurité publique. Ainsi, la transposition en loi française de la directive européenne concernant les données personnelles s'est traduite par une diminution des pouvoirs de contrôle de la Commission Nationale des Libertés (CNIL) sans que cela ait provoqué de remous dans l'opinion. Pour l'auteur, on peut également constater un recul des libertés individuelles dans le domaine des usages de la biométrie ou des projets de cartes d'identité nationale, que l'on a un peu trop tendance à expliquer par les tensions mondiales de l'après 11 septembre 2001. Pour l'auteur, cette acceptation prend une forme plus générale et devient le signe d'une « érosion » du sens du privé et de l'intime dans notre société.

Fabrice Mattatia ne partage pas la vision de Meryem Marzouki. Se concentrant sur le seul projet de carte d'identité électronique – dossier qu'il connaît bien car il en a été l'un des principaux instigateurs au ministère de l'intérieur – l'auteur propose une synthèse complète des avantages et désavantages d'une carte d'identité électronique pour sécuriser

le monde numérique. L'auteur cherche à démystifier certaines critiques souvent énoncées sur les cartes d'identité électronique qui dénotent, selon lui, soit une méconnaissance sur le plan technique, soit une sous-estimation des autres risques encourus en l'absence de déploiement de la carte d'identité numérique.

La contribution de Stéphanie Lacour porte sur la doctrine juridique encadrant les usages des RFID . L'auteur propose une interprétation juridique qui s'appuie sur les avis de la CNIL et sur le contenu de la loi de 1978 « informatique et libertés ». Son raisonnement reprend les dispositions de l'article 2 de cette loi. Les données contenues dans les étiquettes RFID sont-elles des données à caractère personnel ? Et font-elles l'objet d'un traitement ? L'auteur répond par l'affirmative à ces deux questions, ce qui la conduit à définir des obligations aux responsables de ces dispositifs de communication. Si la démarche de l'auteur est louable et constitue l'une des premières tentatives pour faire entrer ces nouvelles technologies dans le droit positif, elle n'en constitue pas moins un exercice périlleux. En effet, il n'existe pas encore de jurisprudence concernant ces technologies, et certaines conclusions de l'auteur reposent sur des prises de positions des membres de la CNIL. Or, si la parole engage, le droit est un langage vivant : ainsi, de grandes innovations juridiques sont nées de revirements impromptus de la Cour de cassation.

C'est un autre aspect de l'écosystème de la confiance qu'observent Benoit Lelong et Céline Metton. Leur texte propose une revue de la littérature anglo-saxonne concernant la protection des enfants face aux nouveaux médias. Ils décryptent les caractéristiques de cette *bedroom culture* consistant à protéger les enfants en les fixant à la maison. Leur analyse consacre une part importante aux conditions de mise en œuvre du contrôle parental en montrant qu'elle nécessite un savoir-faire technique important. Enfin, leur article montre que les technologies numériques tiennent une place importante dans la construction identitaire des enfants – et notamment, des adolescents – et dans leurs stratégies d'autonomisation vis-à-vis des adultes. Ces conclusions conduisent à repenser la manière dont s'exercent – ou doivent s'exercer – le contrôle et la relation parents-enfants, dans un contexte ou la maîtrise technique des outils ne cesse d'augmenter et où l'accès à des contenus devient plus facile, y compris en mobilité.

Les trois dernières contributions sont consacrées au monde de l'entreprise et de la sécurité informatique. Le texte de Dominique Boullier et al. s'intéresse au marché des P.K.I. (*Public Key Infrastructures*) : les auteurs tentent d'expliquer le non décollage de ce marché prometteur. S'inscrivant dans la continuité de travaux en sociologie de l'innovation, les auteurs mettent en avant l'ensemble des médiations nécessaires à l'existence d'une chaîne de sécurité informatique. La nécessité de créer une « ontologie » de la sécurité échoue lorsqu'elle tend à trop vouloir formater les pratiques et les utilisateurs.

Le texte de Chateauraynaud et Trabal concerne un autre volet de la sécurité informatique, celui du monde très fermé des administrateurs de réseaux. Par une méthodologie déjà éprouvée de traitement du corpus à l'aide du logiciel *Prospéro*, les auteurs construisent une sociologie des alertes informatiques leur permettant d'analyser finement le travail de sécurisation effectuée par les administrateurs de réseaux. Ils en concluent que les

administrateurs compétents sont des « vigiles invisibles » pouvant laisser penser que les réseaux fonctionnent sans eux.

Le dossier se conclut par le travail de Nicolas Auray et Danielle Kaminsky qui analyse un autre volet des travailleurs de la sécurité. S'intéressant aux parcours biographiques de virtuoses de l'informatique appartenant à des communautés de *hackers*, les auteurs mettent en évidence quatre trajectoires professionnelles typiques et relève deux paramètres permettant d'expliquer les trajectoires individuelles. Le premier est lié à l'intériorisation d'une éthique professionnelle expliquant de nombreuses reconversions dans le domaine de la sécurité informatique. Le second, plus classique, a trait à leur capital relationnel.

Si ce dossier présente des problématiques de premier plan concernant la sécurité dans un monde numérique, d'autres dimensions auraient pu aussi faire l'objet d'une analyse attentive. Pensons, par exemple, au cas du vote électronique dont l'opinion a pu se rendre compte – aux Etats-Unis lors des Présidentielles de 2000 mais également en France, lors des dernières élections générales – que ce dispositif ne garantissait pas toujours les conditions de la démocratie. Nous n'avons pas non plus évoqué les questions de sécurisation des transactions en ligne, ni celle concernant la e-administration. Peu de choses également sont dites sur la représentation du risque informatique et les dispositifs de sécurisation mis en œuvre par les utilisateurs. La gestion des identités numériques – qui prennent une place croissante avec la montée du Web relationnel dit « Web 2.0 » – aurait mérité également une attention. Espérons que le présent numéro suscitera des vocations de recherche pouvant faire l'objet d'une publication ultérieure sur ce thème très porteur.

Emmanuel Kessous et Serge Proulx

Sommaire :