# Les risques et la sécurité des S.I. : 20 ans après…

## Interview de Daniel Guinier


Daniel Guinier


Gérard Balantzian

**Question 1 : Depuis 1995 et la vulgarisation de l'internet, de l'eau est passé sous les ponts, pour ne pas dire un tsunami… Tu as réalisé un important travail en matière d'expertise, d'enseignement, de conseil et de publication sur le plan de la qualité et de la sécurité des systèmes d'information en France et en Europe. Tu as, en particulier, développé l'approche systémique et des méthodes de spécification et d'audit *: infrastructures à clé publique (PKI), plans de reprise d'activité (PRA), prévus pour des crises extrêmes, etc.* En plus de la recherche et de la veille, tu t'es intéressé aux aspects stratégiques, technico-juridiques et humains de la sécurité, ainsi qu'à l'avancée du droit, et en particulier à la biométrie. Ton intérêt pour la sécurité des SI, en particulier pour la cryptographie, la signature électronique et la preuve numérique, se sont matérialisés par des présentations à des conférences internationales majeures. Le livre *« Catastrophe et management »* de 1995 publié chez Masson n'a-t-il pas été publié trop tôt ?**

**Je le confirme**, mais j'ai toujours été empreint d'un esprit altruiste, considérant qu'**il n'est jamais trop tôt** pour marquer les esprits, susciter des réactions, pour la concrétisation d'actions **avant qu'il ne soit trop tard**. Sans cela, une idée neuve resterait au même stade et sans capacité

d'innovation. C'est ce qui a guidé mes préoccupations, notamment dans les domaines que tu as cités, en privilégiant la vision et les actions positives à long terme.

En 1995, *"Catastrophe et management"* était non seulement le seul livre en Français sur l'urgence et la continuité des SI, mais surtout, il posait des questions de fond, présentait les ingrédients de la **catastrophe**, les enjeux et les conséquences pour l'entreprise. Il apportait un ensemble de réponses de **management** fondées sur des principes et cohérentes pour survivre en cas de crise majeure, tandis que, déjà en période de restriction, il fallait faire des efforts pour éviter des sacrifices causés par des décisions trop tardives et aux dirigeants, de ne pas se voir accuser de *"non-assistance à entreprise en danger".* A cette époque les offres présentaient des *"plans bétonnés"* où de façon rassurante tout était soi-disant établi, sur la base de scénarios prévus, alors qu'il était nécessaire de donner de la souplesse, en mettant l'homme et les processus au centre du dispositif en vue d'une situation imprévisible.

J'ai poursuivi le développement de l'ingénierie systémique des plans de reprise d'activité (PRA) de façon très avancée par rapport aux normes, en me fondant sur la criticité des processus et sur des critères décomposables en termes de fonctionnalités et d'assurances. Aujourd'hui la catastrophe n'est plus considérée comme un mythe et les entreprises s'accordent pour considérer la place du SI de plus en plus cruciale pour les activités dans tous les secteurs, avec une dépendance pressentie comme modérée à forte. Je regrette que, paradoxalement, une grande majorité d'entre elles n'ait pas de réel PRA, sans obligation expresse.

Cet ouvrage a vécu, non sans avoir été relancé, *en particulier après l'accident de l'usine AZF de Toulouse et les attentats du 11 septembre !* Mon précédent livre *"Sécurité et qualité des SI - Approche systémique" de 1991, publié chez Masson*[1]*,* en est un autre exemple encore plus criant. En 1990, le système d'information (SI) était confondu avec la seule informatique, la sécurité réduite au seuil des tous premiers virus, la qualité et la sécurité étaient séparées et l'approche systémique, presqu'une utopie. Avec *"la part de l'homme"* comme sous-titre, cet ouvrage était à la fois un outil théorique, méthodologique et pratique, pour simplifier sans réduire. Depuis ces termes sont usités et la systémique est actuellement en vogue et revendiquée pour être appliquée dans la sécurité des SI, comme il est maintenant affirmé la nécessité de traiter la part de l'homme.

**Il était donc très tôt en tant qu'auteur, mais pas trop tôt pour ouvrir la voie** et être apprécié en tant que consultant pour un bon nombre d'organismes de divers secteurs : *industrie, énergie, aéronautique, télécommunications, transports, santé, recherche, etc.* C'est ainsi que j'ai eu également grand plaisir à enseigner sur ton invitation à l'IMI, l'Institut du Management de l'Information de l'Université de Technologie de Compiègne, au cours de ces 20 années.

**Question 2 : Tu citais en 2005 une phrase d'Hemingway : *"…aux plus importantes croisées des chemins, il n'y a pas de signalisation",* comment faut-il la comprendre face aux risques de l'internet et aux cybermenaces ?**

J'avais en effet utilisé cette phrase dans ma conclusion sur la conception des tableaux de bord, qu'il fallait repenser de façon holistique dans un contexte incertain, pour constituer un instrument-clé pour concourir à des décisions cohérentes dans la gestion de la réponse aux crises ou mieux, dans leur prévention.

Elle suggère ici qu'**il existe bien des chemins** qui pourraient conduire à des atteintes au vu de vulnérabilités intrinsèques **et d'autres qui s'y opposent** par des actions cohérentes associées à divers types de mesures : *prévention, détection, protection, etc.,* en s'appuyant sur la réduction

[1] Dans la collection *Stratégie et Systèmes d'Information* que tu coordonnais.

des déficits en matière de sécurité, pour appliquer efficacement des moyens variés dont certains découlement de l'organisation en se fondant sur l'adhésion des hommes conscients et mieux formés à coopérer et à se défendre. C'est sous ces conditions et par la traduction qui en découle sous forme de tableaux de bord que cette *"signalisation"* attendue se mettra en place pour faire face aux risques de l'internet, au vu des cybermenaces et de la professionnalisation de la cybercriminalité.

**Question 3 : Comme tu le disais en 2005 dans le livre que nous avons rédigé tous ensemble [2] : « *les organismes publics et privés ne peuvent guère se détourner des technologies de l'information et de la communication (TIC)* ». Si « *l'information devient une source de conflit du fait d'enjeux attachés aux connaissances, notamment les plus stratégiques* », comment faut-il faire le tri dans ce chaos informationnel pour comprendre les tendances avant d'agir et d'innover de manière responsable ?**

**Sur le premier point**, *quelle entreprise soumise à la concurrence pourrait se passer de ces technologies?* alors que la visibilité par un site Web, la productivité, la réduction des coûts et des délais sont des éléments de compétitivité, voire même de survie, et que de surcroît, il existe des demandes pressantes liées à l'usage des réseaux sociaux, de moyens personnels (BYOD), du *"cloud computing",* etc., et de divers modes, comme le télétravail et le nomadisme, etc. **Sur le second point**, l'information est radicalement une source de conflit. Des affaires que j'ai pu traiter au plan de l'expertise judiciaire étaient pour beaucoup axées sur le vol ou le détournement de données, impliquant en particulier des PMI/PME. Les révélations d'Edward Snowden montrent une nouvelle fois le visage des nouveaux enjeux de l'information numérique et sa réalité au sein des nations.

**Les enjeux les plus stratégiques** relèvent dès maintenant du *"**Big Data**"* pour **faciliter la prise de décision ou créer un avantage grâce à l'analyse prédictive et contextuelle** qu'il sous-tend. Pour cela, il s'agit de disposer de solutions adaptées qui ont pour objectif de pouvoir traiter un volume gigantesque de données disparates, *structurées ou non.* Elles sont de forme et de nature variées et proviennent de sources diverses : données collectées de *messages, médias sociaux, images et vidéos, transactions, interactions et observations, de divers capteurs,* signaux capturés *de téléphones mobiles, de satellites, etc.* Il s'agit d'**un des grands défis informatiques de la décennie 2010-2020** et une des nouvelles priorités de **recherche et développement**. En présence d'implications encore peu comprises, les organismes doivent s'assurer que l'utilisation du *"Big Data"* est conforme à la législation et aux règlements actuels, en se projetant dans un avenir proche, alors que la mise en œuvre du concept laisse entrevoir des **questions juridiques** au vu de nouvelles solutions techniques non réglementées. Il est cependant à craindre un **déséquilibre de pouvoir entre les tenants de ces technologies** et les Etats comme les entreprises. En particulier, **les PMI/PME manquent souvent de vision et de moyens suffisants**, mais il leur reste néanmoins la capacité de mettre en place une **structure de sécurité et d'intelligence économique**, avec l'aide déjà existante au niveau des territoires, **pour leur permettre d'agir et d'innover** de façon responsable.

**Question 4 : L'innovation au cœur de l'internet est réalisée par des hommes, mais ils ne comprennent pas forcément les conséquences de ce qu'ils inventent, les cercles vicieux ou vertueux autorégulés qui se développent, et l'évolution de la déontologie des relations entre les individus et les machines où le Politique et le Droit s'ajustent sur la réalité qui s'accélère. Par exemple, pour reprendre tes propos, « *l'ambiguïté d'intention relève de motifs et***

[2] (www.lestableauxdebord.com)

***d'objectifs mal définis ou variables au cours du cycle de choix* », et je me souviens que tu disais également « *l'ambiguïté de compréhension résulte d'un environnement méconnu et de technologies obscures ou peu claires. De plus, les choix sont souvent associés à un paradoxe car, d'un côté, les décisions sont considérées comme normales, et de l'autre, comme pathologiques, avec des déficits chroniques* ». Des consortiums sont en train de créer des référentiels qui tenteraient de cadrer et guider les comportements des acteurs nomades qui ne peuvent plus être contrôlés comme hier par la structure pyramide. Des chartes de bonne conduite se propagent partout. Jusqu'où seront-elles respectées à travers par exemple les « lunettes connectées », l'explosion de la circulation planétaire instantanée des contenus numériques, « *la réalité augmentée* » et comment faut-il consolider certaines de nos valeurs pérennes pour co-créer de la valeur ?**

La question précédente et les dérégulations invitent naturellement à celle-ci, en particulier **parce que le cycle des technologies TIC est très court par rapport à l'évolution de la politique et du droit, de la société et des hommes entre eux**. C'est ainsi qu'il se forme diverses ambigüités, dont celles d'intention et de compréhension, avec des conséquences en termes de choix d'organisation, ce qui faisait l'objet de mes recherches aux Etats-Unis en 1983-84 avec James March[3]. A ceci s'ajoutent des décisions à court terme, sans vision ou rigueur et aussi sans suivi, en présence de déficits chroniques non reconnus au sein des organisations et à différents niveaux.

Tout en soulignant leur utilité pour la transmission de la sécurité, comme nous l'avions d'ailleurs montré en 1995[4], **les référentiels comme les guides de bonne conduite à eux-seuls ne sont pas à même de gérer les comportements**, malgré les attentes, les chartes de conduite actuelles ne permettront pas plus de résoudre le contrôle des acteurs nomades dans un cadre de structures transversales, sans être accompagnées d'autres actions pour former la sécurité en profondeur.

**Les technologies TIC représentent une source de création de valeur** par la diffusion des connaissances par le biais du développement de l'internet. Elles ne doivent pas faire oublier que les changements induits suscitent autant de motifs d'inquiétude que d'emballement. Ce ne sont ni les objets connectés, ni l'instantanéité de l'information non vérifiée, qui vont contredire ces faits. Bien au contraire. En fait c'est bien le pouvoir qui est recherché par la maîtrise et la propriété de l'information. Le cas de Google est éloquent à ce propos, si on en juge par les investissements gigantesques tous azimuts, **cherchant à identifier ce que chacun d'entre nous va faire ou va utiliser à l'avenir**, en misant sur l'intelligence et la collecte de données. De fait, si le cyberespace est une fabuleuse place de liberté, **les dérives sont malgré tout inévitables**.

On s'est parfois mépris sur la vocation des outils qui comportent des systèmes et qui sont là pour aider et non pour remplacer l'homme. Ils se développent et intègrent des aspects importants dans les domaines du contrôle, de la prévision, de la fabrication. Ils seront notamment susceptibles de soulager et de réduire les accidents dans un proche avenir. S'il n'en était qu'ainsi **ce serait heureux pour l'humanité**, **mais il faut être vigilent** …

**Nos valeurs pérennes** sont celles de l'humanité et **ma crainte** est celle d'entrer dans une ère nouvelle post-humaine, différente, laissant peu de place à l'individu *"ordinaire"* et donnant pour l'instant l'illusion de coopération au travers de réseaux dits *"sociaux"*. En 1995[5], j'avais insisté sur

[3] Guinier D. (1984) : Tools and organization for a computer methodology in simulation on a model of decision making; application to the *"Garbage Can"* model of Decision making. Joint Workshop on Decision making in Military Organizations, Stanford University - US Naval Postgraduate School, Monterey, 26-28 jan.
[4] Dans le livre *"Catastrophe et management"*, pp. 42-44.
[5] *Ibid*. pp. 48-49.

la **nécessité d'une éthique** présentée sous la forme d'une proposition. **La motion correspondante sous forme de quatre règles simples** avait pour **préalable** que l'humanité, l'environnement et l'être humain ont une valeur supérieure à celle de tout autre système, conformément aux principes d'égalité, d'humanisme et de démocratie de l'OCDE. Se fonder sur ces principes permettrait d'anticiper le fait que la consolidation du **droit ne peut être qu'en retard** en permanence. Elle nécessite du temps et une **vision commune** pour permettre **la coopération internationale**, car ce qui se joue est mondial.

**Question 5 : Je suis d'accord avec toi pour affirmer que les « *déficits en matière de sécurité préexistants sont culturels, avec l'impression d'infaillibilité et une vision simpliste de la sécurité. Les autres sont organisationnels, avec sa subordination à d'autres fonctions et la dilution des responsabilités associées. D'autres enfin sont managériaux, avec l'absence de système de retour d'expérience et de gestion de la sécurité* ». Or, pour se préparer à « l'entreprise 2015 » (et après), quels pièges faut-il dès à présent éviter sur ces trois plans et réussir la transformation numérique ?**

**Ces déficits sont observables avec plus d'ampleur pour les PME/PMI**, précisément à cause d'un manque de perception et de leur persévérance chronique. J'ai pu constater que ces dernières privilégient les moyens techniques et les actions à court terme, en mettant en place le contenu d'une liste comme *"les N commandements"* pratiques, comme dans les années 1990, tandis que les grandes entreprises ont une culture prête à accepter l'apport des sciences du danger et des systèmes à la sécurité, face aux nouvelles menaces. Aussi tant qu'il existera ce sentiment, la sécurité sera en manque d'approche globale et les entreprises seront en quelque sorte comme les *"Shadoks*[6] qui *pompaient, pompaient…* et pensaient à tort que *"ce n'est qu'en essayant continuellement que l'on finit par réussir. Autrement dit : plus ça rate, plus on a de chances que ça marche…".*

Devant ces déficits chroniques malgré les efforts consentis, d'autres approches s'imposent à la compréhension **pour mieux agir et préparer l'entreprise de demain**. Il s'agit de l'**approche par les sciences du danger** pour mettre en évidence des situations déficitaires ou dangereuses et pour déceler des carences, des contradictions, des désorganisations et des blocages, en termes managériaux, organisationnels et culturels[7]. Il s'agit aussi de l'**approche systémique** pour prendre en compte les interactions de différente nature et disposer d'une sécurité ajustée et plus en profondeur, ce qui ressort des offres actuelles, plutôt en direction des grandes entreprises, alors que **les PME/PMI sont pourtant très concernées mais encore malheureusement peu réceptives**, restant précisément dans un cercle non vertueux à cause de ces déficits non reconnus.

En pratique, il s'agit dans ce cadre de **définir la politique de sécurité des SI** et de mettre en relation **le triptyque : hommes-organisation-technologies**, en s'assurant de l'analyse des risques, pour **la sélection** des moyens à mettre en œuvre en respect des normes qui existent pour chacun d'eux. Les tenseurs associés au triptyque relèvent directement de la gouvernance et de la gestion des ressources humaines et du support des TI, tandis qu'ils sont attachés à la culture, au facteur humain et aux architectures. C'est **donc sur cet ensemble qu'il faudrait agir**, ce qui dépasse évidemment la seule application linéaire d'une simple liste de mesures et de moyens à mettre en œuvre.

Interview menée par Gérard Balantzian - 3 avril 2014

[6] Référence au monde des *shadoks*, de la série télévisée d'animation française de 1968 et rediffusée depuis 2010.
[7] Ceci constituait la conférence plénière que j'ai prononcée au 6ème Forum du Rhin supérieur sur les Cybermenaces à Strasbourg (FRC 2013).

# EPILOGUE

***Cher Gérard***

J'ajouterais en guise d'épilogue à notre échange, qu'il n'y a pas lieu d'être fataliste. Il faudrait pourtant abandonner les faux-semblants du pragmatisme et en se servant intelligemment des TIC, imaginer une humanité socialement plus érudite, pour gagner de l'espace et moins haineuse, moins guidée, plus réfléchie, ***plus humaine en quelque sorte***. Ceci éviterait de combler le vide intérieur par bien des artifices voire des addictions et transformations insidieuses qui feraient que deux **individus** *"**vides**"* **de sens n'auraient rien à se dire mais tout à craindre de leur rencontre**, comme c'est souvent le cas de deux *"amis"* d'apparence avec les réseaux sociaux. **Le monde *cyber* devrait appartenir à tous**, **jeunes ou plus âgés**, en se rappelant aussi qu'il est raisonnable d'admettre qu'un message émis d'un *smartphone* ne remplace pas les relations humaines !

***Cher Daniel***

En écho à ton épilogue, je confirme également que la **commutation** numérique ne remplace pas la **communication** humaine. Elles sont complémentaires.