Gestion des risques & COVID-19

REGARD D'EXPERT #4

Mars 2021

René Amalberti

Directeur de la Foncsi

Membre de l'Académie des technologies

Gestion des risques & Covid 19 : imaginer la sécurité de demain

La crise de la Covid-19 et la transformation digitale révèlent-elles les mêmes tendances pour la sécurité de demain ? Quels défis en 2030-2040 ? Témoignage de René Amalberti, directeur de la Foncsi et membre de l'académie des technologies. Ce témoignage est issu du webinaire de l'Icsi du 4 mars 2021.

La crise de la Covid-19 et la transformation digitale révèlent-elles les mêmes tendances pour la sécurité de demain ?

Cela illustre plutôt deux chemins possibles pour la sécurité dans le futur, sans doute faiblement compatibles entre eux.

1er chemin : la résilience systémique

C'est l'héritage historique de la littérature scientifique constituée dans les années 90 par le courant des HRO, puis le courant « resilience engineering ». Cette vision de la sécurité porte l'idée que **les compétences humaines et organisationnelles doivent rester centrales**. Et cette idée se base sur deux points essentiels :

- il faut garder des marges dans le système parce qu'elles permettent de gérer l'inattendu
- il faut savoir se réinterroger chaque jour sur la possibilité d'avoir des surprises et donc ne pas être totalement déterministe.

C'est cette résilience dont on fait preuve pour gérer la Covid et dont le système de santé est une illustration extraordinaire. Si vous allez à l'hôpital et que vous demandez au personnel s'ils doivent suivre les logiques prévues, ils vous diront qu'ils ne peuvent pas parce qu'elles sont inadaptées dans ce contexte de crise. Ils produisent donc de l'intelligence et mettent en œuvre leurs capacités à produire de l'adaptation.

Dans l'industrie, de manière générale, tout ce qui était programmé, algorithmique, prévu éclate avec une immense crise comme celle de la Covid. La sécurité se force alors à **gérer de l'inattendu** et les situations dégradées deviennent la norme.

Ce courant de la résilience permet donc de gérer les situations de **crises, aigues ou chroniques**, pour lesquelles tout ce qui était prévu avant s'avère inadapté et d'avoir de la disponibilité face à l'inattendu. Mais il faut aussi accepter que le niveau de démonstration de gains de sécurité avec une telle approche risque d'être nettement plus difficile pour les cas standards (de loin les plus nombreux).

2e chemin : la révolution digitale

La révolution digitale s'accélère depuis 5 ans et va se poursuivre jusqu'en 2030 -2040. On vit déjà dans un monde algorithmique, dans quelque chose qui veut prévoir avec des outils déterministes. On est ici dans **une vision qui contrôle le système**, qui le garde dans son domaine prévisible grâce à une intelligence digitale adaptative et des puissances de calculs inégalées (big data, intelligence artificielle). On a donc de grandes chances de réduire le risque puisqu'on limite les surprises, mais ce faisant, on réduit la résilience et les postures laissant de l'autonomie et de l'adaptation aux opérateurs et aux managers de tous niveaux.
Il faut reconnaître qu' il existe **un besoin croissant de démonstration de sécurité** dans l'industrie mais également dans la société, pour rassurer les riverains notamment. Ce besoin risque d'imposer au final **cette sécurité digitale** avec sa capacité à **produire de l'indicateur**, à démontrer - dans le domaine prévu et connu - une sécurité extraordinaire, au moins sur le papier. Cette sécurité digitale s'exposera malgré tout aux très grands mais très rares risques que la société connaitra qui sont justement mieux

traités par l'approche précédente de la résilience.

Un autre frein à la poussée du digital pourrait être le phénomène croissant de **désagrégation des entreprises**. Au fil du temps, les entreprises ont expurgé tout ce qui n'était pas central dans leurs composantes industrielles : elles ont constitué des filiales, mis des filiales en compétition entre elles. C'est un processus de création de réseaux d'entreprises y compris internes. Et quand on a la puissance de la sécurité digitale à son service, on va aussi avoir la tentation de produire plus d'indicateurs mais aussi plus de solutions ponctuelles, contextuelles. On aura donc une industrie fragmentée et une sécurité fragmentée qui aura certes de grandes capacités de démonstration mais devra faire face **des défis très importants d'homogénéisation**. Si on a des solutions digitales différentes d'une société à l'autre, il faudra donc aussi une **vision globale**.

Si on se projette en 2030-2040, à quoi ressemble l'opérateur du futur ?

En 2030-2040, nous ferons face à de grands défis qui vont orienter la manière dont on regarde l'opérateur de futur.

Premier défi, nous aurons **3 générations ensemble au travail** qui devront cohabiter : une génération qui reste travailler plus longtemps parce que la retraite est repoussée, une génération intermédiaire et une génération de millénium. Elles auront des aspirations et des vécus différents entre ceux qui sont nés à l'ère du digital et ceux qui ont une ancienneté et des compétences construites avant le digital. Des pays y sont déjà : le Japon a voté la retraite à 70 ans aujourd'hui et à 75 ans en 2025.
On peut imaginer les impacts notamment sur l'évolution des carrières. Les plus anciens seront certainement les grands managers de demain alors que les plus jeunes auront de grandes aspirations en matière d'autonomie ou de reconnaissance de leurs nouvelles compétences. Une des idées pour faire cohabiter les générations est de faire partir les plus anciens de leurs positions managériales pour les mettre dans d'autres positions, comme la formation, et ainsi laisser évoluer les générations qui sont derrière. Et c'est un défi, car la jeune génération ne reconnait pas forcément la compétence de l'ancienne. Au Japon, ils réfléchissent à des formations aux plus anciens pour devenir formateurs des plus jeunes.

Second défi, nous sommes en train de rater en France et en Europe ce que fait bien l'Asie : **la transformation des compétences de nos anciens sur le monde digital**. Notre système de formation continue est en panne : nous ne formons pas assez de jeunes ingénieurs pour répondre aux futurs besoins en matière de sécurité digitale. Nous allons progressivement nous mettre dans une situation de manque de compétences, avec cette fracture des générations dans l'entreprise. Cela laissera place sans doute à des contractualisations et des formations externes.

2030, c'est demain. Nous sommes à un moment clé où nous devrons faire **des virages et préparer l'adaptation de l'entreprise**. Quand on sera face au mur qui va se présenter entre 2025 et 2030, on sera obligé d'accélérer avec beaucoup de douleurs. Il faudrait sans doute mieux s'inspirer des modèles venant d'Asie, même si l'on peut avoir des réponses européennes et françaises différentes. Pour la commission européenne, les métiers technologiques, leurs projections et leurs disponibilités en termes de gestion de carrière en 2030-2040 sont des priorités. C'est également un sujet récurrent de Davos, un vrai sujet de l'organisation de l'entreprise de demain, de la position managériale, de la gestion des carrières et des compétences. Nos systèmes tels qu'ils ont été construits dans les années 2000-2010, sont probablement inadaptés à faire ce saut, contrairement à des systèmes plus jeunes comme ceux de l'Asie ou ceux de l'Afrique. C'est donc un grand défi pour notre culture au-delà d'être un défi technologique et de formation.

Pour en savoir +

>> Replay du webinaire

Retrouvez sur notre chaîne youtube le replay du webinaire « Projection sur le monde de demain » :

>> Suivez la campagne « Gestion des risques & Covid-19 »

L'Icsi questionne la crise de la Covid-19 sous l'angle « crise sanitaire et maîtrise des risques majeurs » et propose un programme de réflexion et d'action autour de 3 axes :
- **un observatoire,**
- **des échanges prospectifs,**
- **un regard sur l'international.**

Découvrez notre rubrique web Gestion des risques & Covid-19

>> Quelques références

Livres
La collection des livres de la FONCSI publiée chez Springer
En anglais, téléchargement gratuit

Site web de l a Foncsi
Analyse stratégique Opérateur du futur