

APPEL À COMMUNICATIONS

Technologies, risques et organisations : vers une nouvelle fabrique des risques ?

Journée d'étude du Groupe Thématique « Risque, Incertitude et Management » de l'AIMS

Vendredi 20 novembre 2026
Paris (lieu précisé ultérieurement)

Les évolutions technologiques sont porteuses d'opportunités, mais elles génèrent également de nouvelles formes d'incertitudes et de vulnérabilités pour les organisations et leurs parties prenantes (Beck, 1992 ; Perrow, 1984). Ces évolutions interrogent les modèles traditionnels de gouvernance et de prise de décision, les rapports de pouvoir, les processus de coordination et les frontières mêmes des organisations (Orlikowski, 2007 ; Zuboff, 2015).

Comme d'autres technologies avant elles, les technologies numériques (intelligence artificielle, blockchain, plateformes numériques, big data, objets connectés, etc.) redéfinissent en profondeur les contours des organisations. Régissant un nombre croissant d'aspects de la vie quotidienne (e-commerce, plateformes de divertissement, dématérialisation des procédures administratives, objets connectés, réseaux sociaux, etc.), le numérique s'impose comme un pilier de l'organisation des infrastructures et des acteurs qui les gouvernent. États, entreprises, citoyens et consommateurs redéfinissent en permanence leur "champ des possibles", au rythme des innovations qui ouvrent la voie à de nouvelles technologies, services et usages. Cette « ère de la digitalisation » renforce l'idée d'une société largement dominée par la technique (Ellul, 1988).

Dans le champ de la gestion des risques, les développements technologiques récents apparaissent à double tranchant (e.g. sur l'IA, Marsden & Steyer, 2025; Endsley, 2023). Les technologies numériques sont porteuses de nombreuses opportunités pour améliorer la gestion des risques. Par exemple, l'anticipation et le pilotage des risques "connus" n'ont ainsi jamais été aussi robustes. Mais de nouveaux risques (Hardy et al., 2020) émergent aussi à mesure que les technologies numériques s'immiscent dans tous les aspects du fonctionnement des organisations. Enfin, l'apparition de nouveaux "objets risqués" (Hilgartner, 1992) - tels que les robots humanoïdes, les plateformes d'accès à l'IA générative ou les véhicules autonomes - soulève des questions inédites de responsabilité et d'éthique (e.g., à qui incombe la responsabilité d'une défaillance ou d'un dommage causé par une IA ?). La régulation de ces enjeux demeure pourtant encore largement embryonnaire.

L'objectif de cette journée d'étude du GT AIMS RIM (Risque Incertitude et Management) est ainsi d'explorer l'impact ambivalent des technologies récentes, notamment des technologies numériques et liées à l'IA mais sans s'y limiter, sur les risques et leur gestion au sein des organisations. Nous invitons ainsi également des travaux souhaitant explorer plus largement l'articulation entre

technologies, risque et résilience. Les travaux présentés lors de cette journée pourront par exemple s'articuler autour des thématiques suivantes (non exhaustives) :

Thème 1. Anticipation et prévention des risques

- Comment les outils prospectifs, tels que les scénarios, intègrent les nouvelles technologies ?
- Quels impacts a le développement de ces technologies sur notre capacité à gérer des horizons temporels différents dans la prévention des risques ?
- Quelles sont les nouvelles méthodes pour appréhender les risques très incertains (e.g., risques environnementaux, risques géopolitiques, risques à très long terme,...) induites par les avancées technologiques ?
- Comment la multiplication des données génère paradoxalement des zones d'ignorance ou d'invisibilisation des risques (biais algorithmiques, données manquantes, opacité des modèles) ?
- ...

Thème 2. Gestion de crise, résilience des organisations et outils digitaux

- Quels rôles jouent les évolutions technologiques, dont le numérique, dans l'anticipation et la réponse aux crises ?
- Comment se structurent les rapports humain-machine dans la gestion des risques ? Comment reconfigurent-ils les dynamiques organisationnelles ? Comment l'abondance d'informations impacte-t-elle les processus de *sensemaking* en situation de crise ? Dans quelle mesure les technologies numériques facilitent ou brouillent la construction de sens partagé au sein des organisations ?
- En quoi les technologies numériques transforment-elles les formes de coordination et les rapports de force dans les processus de gestion de crise ?
- En quoi le numérique, permet-il de structurer une solidarité entre habitants sur des territoires touchés par des catastrophes naturelles ?
- ...

Thème 3. Déploiement des technologies et nouvelles incertitudes

- Quels enjeux éthiques et de régulation les nouvelles technologies introduisent-elles ? Quels processus de construction sociale du risque les sous-tendent ? Comment les incertitudes autour de ces nouvelles technologies sont-elles réduites ou au contraire données à voir dans les controverses qui les entourent ?
- Entre usages détournés, perte de compétences, dévalorisation du travail humain, et déshumanisation des relations sociales, comment ces nouvelles incertitudes bouleversent-elles les secteurs et les métiers ?
- Comment les acteurs ajustent leurs pratiques face à des incertitudes numériques (cyberattaques, défaillances algorithmiques, biais des IA) ?
- Comment appréhender les mécanismes de surveillance, de contrôle ou de dépendance introduits par l'omni-présence accrue des algorithmes ?
- Comment la numérisation transforme-t-elle les dispositifs de valorisation et de mesure du risque (indicateurs, scoring, rating, tableaux de bord automatisés) ? Dans quelle mesure ces instruments participent-ils à une illusion de maîtrise, masquant certaines incertitudes radicales ?
- Comment l'avènement d'un tout-numérique plonge nos sociétés et nos institutions dans un état de vulnérabilité inédit lié à la dépendance aux ressources énergétiques (e.g., risque de

coupe électrique prolongée ou généralisée), et interroge les impacts environnementaux considérables induits par l'augmentation structurelle des besoins numériques ?

-

En parallèle de ces réflexions, cette journée est l'occasion pour notre communauté d'échanger autour de nos travaux. Nous vous invitons donc également à proposer des communications s'intéressant plus largement à la gestion des risques et des incertitudes en contexte organisationnel, dans la mesure où celles-ci visent à renouveler notre compréhension des pratiques et des processus de gestion afférents, et de leurs liens avec le management stratégique des organisations.

Objectifs de la journée

Le groupe thématique encourage les travaux à forte dimension théorique, méthodologique ou empirique, qui proposent de renouveler les approches classiques des formes d'action collective organisée à l'aune des risques et des incertitudes contemporains, en considérant les apports de travaux plus récents. On pourra notamment penser aux travaux s'inscrivant dans les perspectives suivantes (liste non exhaustive) : sensemaking, attention-based view, sociologie pragmatique, valuation studies, approches « practice » variées (avec un intérêt certain pour l'étude de la matérialité), approches discursives/CCO, sociologie des controverses, agnotologie.

Plusieurs types de contribution sont ainsi attendus, qu'ils soient théoriques, méthodologiques, épistémologiques et / ou empiriques, et dès lors qu'ils adressent de manière explicite les notions de risque, d'incertitude, de résilience des organisations.

Afin de permettre une réelle discussion des papiers, le nombre de places, incluant les contributeurs, est limité.

Procédure de soumission

La sélection des communications se fera sur la base d'un résumé étendu, d'une longueur de 3000 mots maximum (bibliographie comprise). Il présentera l'intérêt du sujet, décrira le contenu de l'article et résumera la contribution. Les résumés étendus en anglais sont possibles. Cependant les présentations et les discussions de la journée se feront en français.

Calendrier

- Date limite de soumission des résumés étendus : **20 septembre 2026**
- Retour des avis aux communicants : **5 octobre 2026**
- Envoi de la version finale de la communication : **9 novembre 2026**

Les résumés et les versions finales sont à envoyer par courriel à :
veronique.steyer@polytechnique.edu ; julie.mayer@univ-rennes.fr ;
geoffrey.leuridan@imt-atlantique.fr ; nour.kanaan@univ-lille.fr

Frais d'inscription

La journée ne comporte pas de frais d'inscription. Les frais de transport et de restauration sur place (déjeuner) seront à la charge des participants. Pour les non-adhérents à l'AIMS, il faut y ajouter l'adhésion à l'association (30€, 15€ pour les doctorants) voir <https://www.strategie-aims.com/adherents>

Comité d'organisation de la journée

Véronique Steyer (i3-CRG, Ecole polytechnique), Julie Mayer (CREM, Université de Rennes), Geoffroy Leuridan (IMT Atlantique), Nour Kanaan (Université de Lille).

Références

- Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications, Londres.
- Ellul, J. (1988). *Le bluff technologique*. Hachette, Paris.
- Endsley, M. R. (2023). Ironies of artificial intelligence. *Ergonomics*, 66(11), 1656-1668.
- Hardy, C., Maguire, S., Power, M., & Tsoukas, H. (2020). Organizing risk: Organization and management theory for the risk society. *Academy of management annals*, 14(2), 1032-1066.
- Hilgartner, S. (1992). The social construction of risk objects: Or, how to pry open networks of risk. In J.F. Short and L. Clarke (Eds), *Organizations, uncertainties, and risk* (pp. 39–53). Boulder, CO: Westview Press.
- Marsden E. & Steyer V. (2025), *Artificial intelligence and safety management: an overview of key challenges*. Number 2025-03 of the Cahiers de la Sécurité Industrielle, Foundation for an Industrial Safety Culture, Toulouse, France
- Orlikowski, W. J. (2007). Sociomaterial Practices: Exploring Technology at Work. *Organization Studies*, 28(9), 1435-1448.
- Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press.
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, 30(1), 75-89.