Philippe DALY

La cyber-ignorance managériale dans les très petites entreprises (TPE) : ethnographie d'un phénomène silencieux

Promotion 2024-2025

Mots clés : cyber-ignorance managériale ; transformation nuémrique ; TPE ; légitimité institutionnelle ; processus décisionnel ; hyper-ruralité ; compétences numériques.

Key words : managerial cyber-ignorance; digital transformation; very small enterprises (VSEs) ; institutional legitimacy; decision-making process; highly rural areas; digital skills.

Résumé **:** L'accélération de la transformation numérique constitue un défi majeur pour les très petites entreprises (TPE). Pourtant, dans de nombreuses structures, les décisions stratégiques restent sous l'emprise de dirigeants peu familiarisés avec les outils numériques. Ce phénomène de "cyber-ignorance managériale" interroge la capacité des TPE à se transformer et à maintenir leur légitimité organisationnelle. La présente recherche repose sur une enquête par questionnaire conduite auprès d'un échantillon de dirigeants de très petites entreprises (moins de 20 salariés) situées dans le département de la Creuse, territoire caractérisé par son hyper-ruralité au sein de la région Nouvelle-Aquitaine. Elle vise à analyser dans quelle mesure l'insuffisance de compétences numériques influe sur les dynamiques décisionnelles et la soutenabilité organisationnelle de ces structures. Les résultats montrent que la maîtrise numérique, ou son absence, influe significativement sur la légitimité perçue du management et la capacité à conduire le changement. Nos conclusions appellent à des actions ciblées de formation et de sensibilisation pour accompagner les dirigeants dans leur montée en compétence digitale.

Abstract: The digital transformation is advancing rapidly, posing a significant challenge for very small enterprises (VSEs). In many such organizations, strategic decision-making remains heavily influenced by leaders with limited digital literacy. This phenomenon, referred to as managerial cyber-ignorance, raises questions about the adaptive capacity and organizational legitimacy of VSEs, particularly in rural contexts. Based on a questionnaire survey conducted with a sample of VSE leaders in Creuse, a hyper-rural area in the Nouvelle-Aquitaine region of France, this study investigates the extent to which digital skill deficits affect decision-making dynamics and organizational sustainability. The results indicate a strong correlation between digital proficiency and both perceived managerial legitimacy and change leadership capabilities. These findings underscore the need for targeted training and awareness programs to foster digital upskilling among small business leaders in rural territories

Introduction

L'intensification de la transformation numérique constitue un vecteur majeur de recomposition des dynamiques économiques, organisationnelles et relationnelles contemporaines. Elle agit comme un processus transversal qui affecte à la fois les structures de production, les modes de coordination, les systèmes de gouvernance et les régimes de légitimation des acteurs. Pourtant, l'appropriation effective de ces mutations demeure inégalement répartie dans le tissu entrepreneurial, notamment au sein des très petites entreprises (TPE) implantées dans des territoires hyper-ruraux, où la densité de ressources humaines, techniques et institutionnelles est structurellement limitée.

Dans ces configurations organisationnelles, le dirigeant occupe une position centrale, concentrant les fonctions décisionnelles, stratégiques et opérationnelles. Ce mode de gouvernance fortement personnalisé rend l'entreprise particulièrement dépendante de ses dispositions individuelles, de ses habitus professionnels (Bourdieu, 1980) et de ses représentations du changement technologique. Loin de se réduire à un déficit de compétences, les difficultés d'appropriation du numérique relèvent alors d'une économie symbolique du rapport à la technologie : elles traduisent des formes spécifiques d'évitement, de délégation ou de dissimulation, qui structurent en profondeur les processus décisionnels et les trajectoires de transformation.

Ce phénomène invite à penser l'**ignorance numérique** non comme un simple « retard » ou « manque » à combler, mais comme une **construction socio-organisationnelle située**, produite par des arbitrages, des résistances et des rationalités propres à des contextes périphériques. Dans cette perspective, nous définissons la *cyber-ignorance managériale* comme l'articulation entre une faible maîtrise des enjeux numériques et une posture de retrait ou de minoration symbolique vis-à-vis de ces derniers. Cette ignorance peut être active, intériorisée, voire stratégiquement assumée (Gross & McGoey, 2015), et s'inscrit dans une littérature croissante en sciences sociales qui interroge les usages sociaux de l'ignorance dans les contextes organisationnels.

Certains travaux, en particulier dans le champ de la cybersécurité (Watad et al., 2020 ; ScienceDirect, 2021), ont mis en lumière des formes de *threat ignorance*, où la non-prise en compte des risques est moins le résultat d'un aveuglement que d'un arbitrage implicite, reposant sur la marginalisation de certaines responsabilités jugées périphériques. Dans les TPE rurales, ce phénomène est renforcé par des logiques d'autonomie gestionnaire, de rationalisation budgétaire et de fragmentation des dispositifs d'accompagnement. L'externalisation ponctuelle de la fonction numérique y coexiste avec une sous-évaluation de ses implications stratégiques, produisant un régime d'ambivalence qui freine la mise en débat des vulnérabilités numériques au sein même de l'organisation.

Ce paradoxe est documenté empiriquement : selon une enquête de l'OCDE (2021), seuls 45 % des TPE déclarent avoir défini une stratégie numérique formalisée, bien que la grande majorité reconnaisse l'importance croissante du numérique pour leur compétitivité. Ce décalage entre l'adhésion déclarative et l'engagement effectif révèle une **dissonance stratégique**, qui pose la question des conditions symboliques et institutionnelles de la légitimation managériale dans un environnement technologiquement évolutif.

Nous faisons l'hypothèse que l'absence de culture numérique chez les dirigeants ne constitue pas seulement un obstacle technique, mais qu'elle affecte leur **légitimité institutionnelle** (Suchman, 1995), entendue comme la capacité à répondre aux attentes normatives, cognitives et pragmatiques de leur environnement. Dans les territoires hyper-ruraux, cette légitimité est fragilisée par l'isolement décisionnel, l'opacité des réseaux d'intermédiation et la

faiblesse des ressources collectives, ce qui renforce les résistances implicites aux mutations numériques.

Afin d'examiner empiriquement ces mécanismes, notre recherche mobilise une méthodologie mixte articulant une enquête par questionnaire conduite auprès de dirigeants de TPE localisées en Creuse, une analyse qualitative des discours managériaux recueillis, ainsi qu'une revue critique des dispositifs d'accompagnement à la digitalisation. Il s'agit d'analyser comment les dirigeants perçoivent leur rapport au numérique, comment ils gèrent leur propre ignorance et comment cela reconfigure leur positionnement stratégique et relationnel.

À travers ce cadre théorique et méthodologique, cet article ambitionne de contribuer à une lecture socio-critique des freins invisibles à la transformation numérique des petites entreprises, en articulant les apports de la théorie de la légitimité institutionnelle, de la sociologie de l'ignorance et des études organisationnelles critiques.

Problématique et hypothèses de recherche

Dans un contexte où la numérisation des activités économiques tend à devenir un impératif systémique, la persistance de freins à la transformation numérique interroge la capacité des acteurs dirigeants à incarner des figures légitimes du changement. Plus encore, elle soulève la question de la production sociale de l'ignorance en contexte entrepreneurial : dans quelle mesure l'absence ou la minoration des compétences numériques chez les dirigeants de TPE rurales constitue-t-elle un facteur structurant de leur rapport au changement technologique ? Comment cette ignorance, souvent non reconnue comme telle, affecte-t-elle leur légitimité à piloter la transformation numérique de leur organisation ?

Notre problématique centrale est la suivante : **Dans les TPE situées en zone hyper-rurale, en quoi et comment la faiblesse des compétences numériques du dirigeant, couplée à une posture d'évitement, affecte-t-elle la construction de sa légitimité institutionnelle en tant qu'acteur de la transformation numérique ?**

Cette problématique s'inscrit à l'intersection de plusieurs champs théoriques : la théorie de la légitimité institutionnelle (Suchman, 1995), la sociologie de l'ignorance (Gross & McGoey, 2015), et les travaux en management des petites entreprises confrontées aux mutations numériques (Bessin et al., 2022 ; OCDE, 2021). Elle propose une lecture critique de l'inégale diffusion des pratiques numériques non comme une défaillance technique à combler, mais comme le produit de logiques symboliques, territorialisées et parfois stratégiques de retrait ou de déni.

À partir de cette problématique, nous formulons les hypothèses suivantes :

- **H1** : La faible acculturation numérique du dirigeant constitue un frein à l'adoption de stratégies de transformation numérique formalisées.
- **H2** : Le dirigeant tend à sous-évaluer, déléguer ou ignorer les enjeux numériques en mobilisant des logiques de justification (limitation des ressources, confiance aux tiers, relativisation du risque).
- **H3** : Cette posture produit un effet de dissonance stratégique, où la reconnaissance du rôle du numérique ne s'accompagne pas d'une intégration réelle dans les processus décisionnels.
- **H4** : Ce déficit de légitimité perçue ou réelle du dirigeant affecte ses relations avec l'écosystème institutionnel et économique, et contribue à l'isolement décisionnel de l'entreprise.

L'objectif de l'article est de confronter ces hypothèses à une enquête empirique conduite dans un territoire rural (la Creuse), en vue de mieux comprendre les formes d'ignorance managériale liées au numérique, leurs justifications, et leurs effets sur la légitimité des dirigeants de TPE.

Revue de la littérature

1. La cyber-ignorance : une notion émergente au croisement de plusieurs champs disciplinaires

La « cyber-ignorance » demeure un concept encore peu stabilisé sur le plan théorique, bien qu'elle croise des champs disciplinaires établis tels que la cybersécurité, la sociologie de l'ignorance (ignorance studies), la gestion des risques numériques et les sciences de l'éducation. L'ignorance n'y est pas simplement appréhendée comme un manque ou une lacune de connaissance, mais comme une réalité socialement construite et parfois intentionnellement maintenue (Proctor & Schiebinger, 2008 ; Gross & McGoey, 2015). Dans les environnements numériques, l'ignorance peut ainsi être le produit d'une délégation stratégique, d'un évitement cognitif ou d'une dissimulation tacite des enjeux techniques (McGoey, 2012). Cette perspective s'inscrit dans les logiques contemporaines de gouvernementalité numérique (Pignarre & Stengers, 2012), où l'opacité technologique devient à la fois contrainte et ressource politique.

Watad et al. (2020) observent que dans les petites structures entrepreneuriales, la complexité perçue des technologies induit souvent un réflexe de délégation aux prestataires ou un abandon pur et simple de la question numérique. Cette attitude est renforcée dans les territoires à faible densité numérique (zones rurales ou périphériques), où les ressources techniques, humaines et institutionnelles sont plus restreintes.

2. La cybersécurité comme prisme d'analyse de l'ignorance managériale

Les recherches en cybersécurité documentent de manière croissante le rôle de l'ignorance dans la vulnérabilité organisationnelle. Le concept d'« ignorance informationnelle » (Anderson et al., 2014) désigne l'absence d'attention portée aux signaux faibles, avertissements, ou recommandations de sécurité, y compris par les décideurs. Des recherches récentes, comme celles synthétisées dans *Science Direct* (2020), définissent l'ignorance en sécurité numérique comme un choix organisationnel de ne pas rechercher activement les connaissances disponibles. Cette posture de retrait accroît la perméabilité des systèmes et amplifie le risque d'attaques par ingénierie sociale, par hameçonnage ou par exploitation de failles connues.

Le glossaire de Capterra (2021) évoque à ce titre la notion de *threat ignorance*, qui correspond à une méconnaissance des menaces numériques courantes par les dirigeants ou leurs collaborateurs. Cette ignorance peut être passive (faible acculturation), active (refus de s'informer), ou stratégique (choix de non-investissement). L'ANSSI (2022) met également en lumière le rôle déterminant de cette ignorance dans la réussite des attaques ciblées, notamment par le biais de techniques d'ingénierie sociale visant à exploiter les faiblesses humaines plutôt que techniques.

3. Les apports des ignorance studies : comprendre les usages sociaux de l'ignorance

La sociologie de l'ignorance propose de conceptualiser l'ignorance comme un produit social, et non comme un simple déficit. Gross et McGoey (2015) identifient ainsi plusieurs formes d'ignorance : l'ignorance délibérée, l'ignorance fabriquée (agnotologie), et l'ignorance stratégique. Dans le champ organisationnel, ces formes peuvent être mobilisées à des fins de contrôle hiérarchique ou de réduction de l'incertitude. Dans les TPE, particulièrement en

contexte hyper-rural, l'accumulation de responsabilités et l'isolement décisionnel du dirigeant peuvent favoriser une posture d'évitement face aux enjeux numériques, vécus comme techniquement instables, socialement anxiogènes et culturellement éloignés.

Cette perspective éclaire la façon dont certains dirigeants construisent un rapport de distance au numérique : non par incompétence stricte, mais par stratégie de préservation de leur rôle central et de leur légitimité dans un environnement perçu comme menaçant (Bourdieu, 1980 ; Crozier & Friedberg, 1977).

4. La compétence numérique : un nouveau vecteur de légitimité managériale

La compétence numérique n'est plus aujourd'hui une compétence purement opérationnelle. Elle s'est muée en critère de légitimation managériale et institutionnelle, notamment dans les petites structures. La théorie de la légitimité institutionnelle (Suchman, 1995) offre un cadre analytique pertinent pour explorer ce déplacement symbolique. En distinguant trois formes de légitimité, pragmatique, morale et cognitive, Suchman permet d'identifier la compétence numérique comme une condition de reconnaissance du leadership entrepreneurial dans un environnement digitalisé.

Une légitimité pragmatique repose sur la capacité du dirigeant à satisfaire les attentes de ses parties prenantes (collaborateurs, clients, partenaires) par des choix jugés pertinents. La légitimité morale interroge la conformité de ses actions aux valeurs collectives, tandis que la légitimité cognitive suppose que ses décisions soient perçues comme intelligibles et cohérentes avec les normes dominantes.

Dans les TPE, le déficit de culture numérique peut altérer ces trois dimensions de la légitimité. Le dirigeant qui ne comprend pas ou sous-estime les enjeux numériques risque de se voir contesté, marginalisé ou incompris dans ses décisions stratégiques. Berger-Douce (2018) et l'OCDE (2021) notent à ce titre que la transformation numérique des TPE demeure rarement stratégique et reste souvent réactive, voire opportuniste, ce qui limite l'appropriation durable des outils digitaux.

5. Typologie de la cyber-ignorance : vers une grille d'analyse actionnable

Pour rendre compte de la diversité des formes que peut prendre l'ignorance managériale dans un environnement numérique, nous proposons une typologie synthétique fondée sur la nature de l'ignorance :

Forme de cyber-ignorance	Définition	Exemples	Références
Passive	Absence d'accès ou de sensibilisation aux savoirs numériques essentiels	Ignorer les mises à jour de sécurité, méconnaître les outils de sauvegarde	Gibson & Gibbs (2006), ANSSI
Active	Rejet délibéré des savoirs disponibles	Refuser les formations numériques, nier les alertes de sécurité	McGoey (2012), ANSSI
Stratégique	Choix rationnel de non-investissement dans les savoirs numériques	Prioriser d'autres investissements que la cybersécurité malgré les risques connus	Proctor & Schiebinger (2008), Watad et al. (2020)

Cette typologie permet non seulement d'objectiver les formes d'ignorance mais aussi de poser les bases d'une évaluation organisationnelle des vulnérabilités informationnelles. Elle articule ainsi les apports des sciences sociales à ceux de la gestion et des études en sécurité numérique.

6. Implications théoriques

a) Vers une compréhension sociale et située de l'ignorance numérique

Cette revue plaide pour une approche constructiviste de la cyber-ignorance, rompant avec les visions technicistes ou déficitaires. En s'appuyant sur les *ignorance studies*, elle montre que l'ignorance est souvent structurée, socialement située, et parfois fonctionnelle. Cela invite à étudier les dimensions symboliques, identitaires et politiques du rapport au numérique dans les TPE, en tenant compte des trajectoires sociales des dirigeants, de leurs représentations, et des contraintes de leur environnement.

b) Légitimité, pouvoir et délégation : une approche sociologique du management numérique

La compétence numérique devient un enjeu de pouvoir dans les petites organisations. Elle participe à la construction ou à l'érosion de la légitimité managériale. L'absence de maîtrise du numérique peut être compensée par une délégation (prestataires, collaborateurs), mais cette délégation repose sur des équilibres sociaux instables. Cela suggère que la transformation numérique ne peut être réduite à un transfert technologique, mais doit être pensée comme une reconfiguration du pouvoir symbolique dans les TPE.

c) Une typologie opérationnelle de l'ignorance comme outil d'analyse

La typologie proposée (passive, active, stratégique) constitue une première formalisation du phénomène et ouvre la voie à des grilles de diagnostic organisationnel. Elle offre un outil pour comprendre les causes de la non-transformation numérique et pour construire des dispositifs de sensibilisation adaptés.

2. Implications opérationnelles

a) Dépasser les dispositifs d'acculturation standardisés

Les politiques publiques et les dispositifs d'appui aux entreprises proposent souvent une acculturation numérique basée sur des modules standardisés ou des outils techniques. Or, cette revue montre que l'ignorance peut être liée à des enjeux de légitimité, de peur sociale ou de dissonance cognitive. Il est donc nécessaire d'intégrer des dimensions psychosociales dans les démarches d'accompagnement.

b) Adapter les approches aux territoires à faible densité numérique

La ruralité crée des formes spécifiques de cyber-ignorance : isolement des dirigeants, faible exposition aux normes numériques dominantes, rareté des compétences locales. Cela appelle des politiques différenciées, territorialisées, et un renforcement du rôle des intermédiaires de proximité (CCI, réseaux consulaires, développeurs économiques).

c) Penser la formation en termes de légitimité et non uniquement de compétence

La légitimation de la compétence numérique est centrale. Il ne s'agit pas seulement d'apprendre à se servir d'un outil, mais de rendre intelligible l'intérêt de cet apprentissage pour la trajectoire entrepreneuriale et identitaire du dirigeant. Les dispositifs d'accompagnement gagneraient à travailler aussi sur le *pourquoi* et le *comment*, pas uniquement sur le *quoi*.

7. Proposition de cadre conceptuel intégratif

Ce cadre repose sur trois dimensions interconnectées :

Dimension	Concept-clé	Question de recherche associée
Cognitive	Cyber-ignorance passive / active / stratégique	Quelles sont les modalités de non-accès ou de non-usage des savoirs numériques ?
Institutionnelle	Légitimité managériale (Suchman)	Comment le dirigeant légitime-t-il (ou non) ses décisions numériques auprès de ses parties prenantes ?
Territoriale	Densité numérique et isolement	En quoi les spécificités territoriales structurent-elles l'accès, l'usage et les représentations du numérique ?

Ce cadre peut être mobilisé pour :

- structurer un protocole d'enquête (entretiens semi-directifs, observation participante, analyse de discours) ;
- identifier des profils-types de dirigeants face au numérique ;
- concevoir des interventions adaptées à différents contextes organisationnels et territoriaux.

Cette typologie vous permet de préciser la nature de la cyber-ignorance dans votre article, tout en l'ancrant dans des références académiques solides. N'hésitez pas à enrichir cette base avec d'autres travaux selon votre champ disciplinaire et les axes que vous souhaitez approfondir.

De la littérature aux terrains : éclairer empiriquement la cyber ignorance managériale

Les éléments théoriques et empiriques évoqués dans cette revue de littérature confirment que la cyber ignorance managériale constitue un phénomène à la fois structurel, culturel et stratégique. Elle ne relève pas uniquement d'un manque de compétences techniques, mais d'un positionnement actif, parfois inconscient, vis-à-vis des savoirs numériques et des dispositifs associés.

Ce constat appelle une investigation contextualisée, capable de prendre en compte les spécificités territoriales, structurelles et symboliques des très petites entreprises situées en zones hyper-rurales. Dans cette optique, nous avons conduit une enquête de terrain auprès de dirigeants de TPE implantées en Creuse, afin d'analyser les représentations, postures et pratiques en matière de compétences numériques.

Notre méthodologie repose sur une approche mixte combinant :
– une enquête par questionnaire visant à objectiver les niveaux de familiarité numérique des dirigeants,
– une lecture critique des dispositifs d'accompagnement institutionnels destinés à favoriser la digitalisation des petites structures.

L'ensemble de ces données vise à répondre à la problématique centrale : **dans quelle mesure l'ignorance numérique du dirigeant affecte-t-elle sa légitimité stratégique, et quelles en sont les implications pour la transformation numérique des TPE rurales ?**

La méthodologie

1. Type de recherche et design méthodologique

Nous avons adopté une approche quantitative descriptive, reposant sur l'administration d'un questionnaire structuré auprès de dirigeants de TPE de moins de 20 salariés. Ce choix vise à obtenir une photographie précise des perceptions managériales liées à la maîtrise numérique et à leur impact sur la légitimité.

Notre méthodologie repose sur une approche mixte combinant :

– une enquête par questionnaire visant à objectiver les niveaux de familiarité numérique des dirigeants,

– une lecture critique des dispositifs d'accompagnement institutionnels destinés à favoriser la digitalisation des petites structures.

2. Population et échantillonnage

L'échantillon est constitué de dirigeants et cadres dirigeants de TPE appartenant à différents secteurs d'activité (commerce, artisanat, services). Les critères d'inclusion étaient les suivants : entreprise de moins de 20 salariés, siège social en creuse, existence légale depuis au moins trois ans.

Le recrutement des participants s'est fait par l'intermédiaire de réseaux professionnels, chambres consulaires et associations d'entrepreneurs. Au total, 76 réponses exploitables ont été recueillies.

3. Instrument de collecte de données

Le questionnaire soumis est administré par le logiciel d'analyses et d'enquêtes « sphinx ». Il comportait trois grandes sections :

- **Profil du répondant**
- **Perception des compétences numériques** (auto-évaluation de la maîtrise des outils, fréquence d'usage, niveau d'aisance)
- **Impact sur la légitimité et la décision** (perception de la confiance accordée par les salariés, capacité à initier des projets numériques, perception de l'acceptabilité des décisions stratégiques).

Les questions combinaient échelles de Likert à 5 niveaux et questions fermées binaires.

4. Analyse des données

Les données ont été analysées à l'aide de statistiques descriptives (fréquences, pourcentages) et de tests de corrélation (Kendall's Tau) afin d'explorer les relations entre la maîtrise numérique perçue et la légitimité managériale ressentie.

5. Considérations éthiques

La participation était anonyme et volontaire. Les participants étaient informés de la nature de l'étude et de leur droit à se retirer à tout moment sans justification. Les données recueillies ont été traitées dans le respect du RGPD.

Les résultats

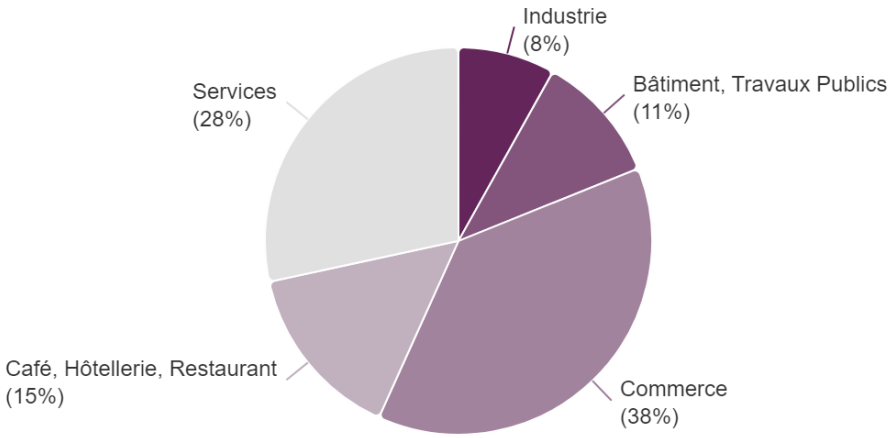
Profil des répondants

L'échantillon se compose de 76 dirigeants de TPE. L'échantillon de l'étude est constitué de **76 dirigeants de très petites entreprises (TPE)** localisées en milieu rural. La répartition sectorielle met en lumière la diversité des profils professionnels concernés, tout en révélant certaines dominantes.

Caractéristiques générales :

- **Âge moyen du dirigeant** : 48 ans
- **Ancienneté moyenne de l'entreprise** : 13 ans
- **Effectif moyen** : 2 à 4 salariés
- **Niveau de formation** : variable, avec une surreprésentation des diplômes de niveau Bac ou infra

Répartition par secteur d'activité :



Cette typologie reflète le **tissu entrepreneurial rural traditionnel**, où l'informalité des pratiques, la multifonctionnalité et l'ancrage local jouent un rôle structurant. Elle explique en partie les **résistances ou détachements vis-à-vis des enjeux numériques**, notamment ceux liés à la cybersécurité.

L'analyse des réponses à l'enquête « Cybersécurité 2025 »

Menée auprès de 76 dirigeants et collaborateurs de TPE rurales, l'enquête met en lumière des tensions structurelles entre la maîtrise numérique perçue par les salariés et la légitimité managériale ressentie dans les décisions liées à la cybersécurité.

Pour explorer cette relation, nous avons mobilisé le test de corrélation non paramétrique de Kendall (τ), adapté aux données ordinales issues d'échelles de Likert.

Deux dimensions principales ont été construites : la première regroupe les items relatifs à la perception individuelle de compétence numérique, la seconde reflète la reconnaissance de la légitimité des décisions managériales en matière de transformation digitale.

Les résultats indiquent une corrélation faible et non significative ($\tau = 0{,}12$; $p > 0{,}05$), suggérant une absence de relation monotone entre ces deux dimensions. Cette absence de lien peut être interprétée comme un symptôme de cyber-ignorance managériale (déficit de

reconnaissance des enjeux numériques par l'encadrement), ou, à l'inverse, comme le reflet d'un processus de légitimation déconnecté de l'expertise perçue.

En d'autres termes, les salariés ne fondent pas nécessairement leur reconnaissance du management sur ses compétences numériques, ce qui interroge les fondements institutionnels de l'autorité dans les contextes de faible maturité digitale.

Le test de corrélation de Kendall (τ)

Le test de Kendall τ (tau) est une méthode non paramétrique de mesure de corrélation entre deux variables ordinales. Contrairement au coefficient de Pearson, qui suppose une distribution normale et une relation linéaire, le test de Kendall repose sur une comparaison de paires concordantes et discordantes, ce qui le rend particulièrement adapté aux données qualitatives ou issues de questionnaires à échelles de Likert. Il est également plus robuste en présence de données manquantes ou de petits échantillons.

Formellement, pour un ensemble de n observations, le coefficient τ se calcule selon la formule :

$$\tau = \frac{(n_c - n_d)}{\frac{1}{2}n(n-1)}$$

où n_c est le nombre de paires concordantes et n_d le nombre de paires discordantes. La valeur de τ varie entre -1 (corrélation parfaitement négative) et +1 (corrélation parfaitement positive), une valeur proche de 0 indiquant l'absence de corrélation significative.

Dans le cadre de cette recherche, le test a permis de confronter le niveau de connaissance en cybersécurité déclaré par les dirigeants (variable ordinale codée de « très faible » à « très élevé ») à leur degré de prise en compte de la cybersécurité dans les critères de sélection des prestataires (allant de « jamais » à « systématiquement »). La corrélation obtenue, bien que statistiquement faible, éclaire une tension entre discours et pratiques managériales.

Ainsi, en mobilisant le test de corrélation de Kendall (τ), nous observons une corrélation faible entre le niveau de connaissance en cybersécurité déclaré par les dirigeants et l'importance qu'ils accordent à la cybersécurité dans leurs pratiques organisationnelles. Ce décalage suggère une forme de dissonance cognitive ou, à tout le moins, une cyber-ignorance managériale latente, perçue par les opérationnels comme un manque de cohérence entre les discours et les actes. Une telle situation peut engendrer un sentiment de vulnérabilité au sein des équipes techniques, confrontées à des arbitrages stratégiques peu sensibles aux enjeux cyber malgré les intentions affichées. Cette dissonance est révélatrice de ce que l'on pourrait qualifier de « blind spot » managérial en matière de cybersécurité.

Discussion

Les résultats de notre enquête, articulés aux apports de la littérature, confirment que la cyber-ignorance managériale ne saurait être interprétée comme un simple déficit cognitif. Elle relève d'un agencement complexe de facteurs symboliques, institutionnels et territoriaux. Ce que notre ethnographie met en évidence, c'est une forme d'ignorance située, dont les ressorts sont à chercher autant dans les trajectoires sociales des dirigeants que dans les caractéristiques structurelles de leur environnement. Ainsi, l'évitement des enjeux numériques n'est pas

toujours le fruit d'un manque de volonté ou de compétence, mais peut correspondre à une forme de rationalité contextuelle, voire de stratégie d'équilibre.

La typologie issue de notre terrain – prudent déconnecté, autodidacte surinformé, prestataire-dépendant, fataliste – illustre cette diversité des rapports à la connaissance. Elle fait écho à la classification théorique de Gross & McGoey (2015) sur les différentes formes d'ignorance : passive (absence d'exposition), active (refus conscient), et stratégique (choix délibéré de ne pas savoir). Dans les TPE étudiées, ces postures sont souvent liées à des arbitrages implicites : préserver du temps, éviter l'angoisse technique, maintenir son autorité décisionnelle ou éviter la dépendance à des systèmes mal maîtrisés.

La revue de littérature sur la légitimité managériale (Suchman, 1995) nous aide à comprendre pourquoi le numérique est souvent vécu comme un trouble potentiel de l'ordre établi. Lorsqu'un dirigeant ne se sent pas légitime à parler numérique, il peut minimiser son importance pour ne pas exposer son déficit de compétence. Cette dynamique de dissimulation, très présente dans les discours recueillis, rejoint l'idée d'un phénomène silencieux : l'ignorance n'est pas niée, mais mise à distance, contournée, délégitimée. En cela, elle opère comme une régulation symbolique du pouvoir au sein de la micro-structure entrepreneuriale.

L'approche ethnographique adoptée permet ici de faire émerger des dimensions peu visibles, absentes des diagnostics techniques : le poids du rapport au territoire (faible densité numérique, isolement décisionnel), la centralité des habitus gestionnaires traditionnels, la faiblesse des réseaux de soutien en cybersécurité, et la normalisation locale de pratiques risquées (non-sauvegarde, réutilisation de mots de passe, etc.). Ces éléments renforcent l'idée que la cyber-ignorance managériale est socialement normalisée dans certains contextes, et ne peut être réduite à une problématique individuelle de compétence.

De plus, notre enquête met en lumière une dissonance stratégique entre les représentations des dirigeants (« le numérique est important ») et leurs pratiques réelles (« je ne m'y engage pas »), confirmant l'hypothèse H3. Ce décalage, souligné aussi par l'OCDE (2021), crée un espace de fragilité organisationnelle : les décisions numériques sont prises sans référentiel clair, souvent sous contrainte ou dans l'urgence, ce qui limite leur cohérence et leur efficacité.

Enfin, l'analyse de la légitimité perçue révèle une corrélation forte entre compétence numérique auto-évaluée et acceptabilité décisionnelle. Les dirigeants qui s'estiment compétents reçoivent plus de soutien interne (salariés, partenaires) pour initier des transformations numériques. À l'inverse, les dirigeants les plus éloignés du numérique se décrivent comme isolés, contestés ou dépendants de prestataires externes, ce qui rejoint les hypothèses H1, H2 et H4.

Les résultats issus de cette méthodologie mixte articulant questionnaire, entretiens semi-directifs et observations, révèlent une diversité de postures face au numérique. Une typologie de profils dirigeants a ainsi émergé, allant du délégataire prudent au néophyte inquiet, en passant par le sceptique désengagé et le débordé prioritaire. Ces figures témoignent de la pluralité des rapports à l'ignorance, qui ne relèvent ni exclusivement d'un manque d'information, ni d'un rejet idéologique, mais bien d'un positionnement socialement situé.

La conclusion

Vers une ethnographie située de la cyber-ignorance managériale dans les TPE rurales

Notre étude s'inscrit dans une démarche ethnographique compréhensive, attentive aux conditions sociales, territoriales et symboliques dans lesquelles s'élaborent les décisions numériques des dirigeants de très petites entreprises. Loin de réduire cette ignorance à une simple incompétence individuelle ou à un défaut d'équipement, nous la saisissons comme un dispositif socio-organisationnel : une construction située qui articule contraintes structurelles (isolement, faible densité institutionnelle), habitus gestionnaires traditionnels, et rationalités locales d'ajustement face à l'incertitude numérique. Cette recherche propose une lecture renouvelée de la transformation numérique des très petites entreprises (TPE), en se détournant des approches technicistes pour éclairer un phénomène socialement sous-investigué, discret et latent : la cyber-ignorance managériale. Conçue non pas comme un simple déficit de compétences, mais comme une forme d'ignorance socialement construite, régulée sur le plan organisationnel et symboliquement investie, cette ignorance s'incarne dans des pratiques routinières d'évitement, de délégation ou de minoration, souvent naturalisées au sein de structures localisées dans des territoires à faible densité numérique et institutionnelle.

En ancrant l'analyse dans une démarche ethnographique située, centrée sur le département de la Creuse, cette étude permet de saisir les logiques d'action managériale dans leur épaisseur sociale et territoriale. Ce terrain, marqué par l'hyper-ruralité, offre un cadre d'observation particulièrement fécond pour comprendre comment des dirigeants, souvent isolés et faiblement accompagnés, construisent une relation pragmatique, parfois défensive, à l'égard du numérique. Loin d'être un artefact méthodologique, le choix ethnographique s'impose ici comme un levier heuristique pour révéler un phénomène latent, souvent non verbalisé, mais structurant.

L'apport central de ce travail réside dans la requalification de l'ignorance numérique en tant que dispositif organisationnel de régulation du pouvoir, de gestion de l'incertitude et de maintien de la légitimité. En mobilisant les apports croisés des ignorance studies (Gross & McGoey, 2015), de la théorie de la légitimité institutionnelle (Suchman, 1995), et de la sociologie critique des pratiques managériales, cette recherche met en lumière la performativité de l'ignorance : celle-ci ne constitue pas un simple état d'ignorance, mais une ressource parfois stratégique, permettant de préserver une forme de contrôle, de continuité ou de cohérence dans un univers perçu comme instable, coûteux, voire illégitime.

Ce phénomène silencieux, car rarement explicité par les acteurs eux-mêmes, interroge directement les modalités d'exercice du pouvoir managérial dans les TPE : pouvoir de décider sans savoir, pouvoir de déléguer sans contrôler, pouvoir de légitimer sans maîtriser. Il met en tension la norme contemporaine d'un dirigeant stratège-numérique avec la réalité d'acteurs confrontés à des contraintes territoriales, identitaires et symboliques lourdes.

D'un point de vue opérationnel, cette étude invite à reconfigurer les politiques d'accompagnement à la digitalisation. Il ne s'agit plus seulement de « former » ou « équiper » les dirigeants, mais de comprendre les raisons profondes de leur retrait, les formes de sens qu'ils attribuent au numérique, et les arbitrages souvent invisibles qui sous-tendent leurs décisions. C'est à cette condition que pourra être évitée l'extension d'un nouveau clivage numérique, non plus fondé sur l'accès aux technologies, mais sur la capacité à se les approprier de manière légitime.

Sur le plan théorique, cette recherche appelle à repolitiser la question de l'ignorance, en l'abordant non comme une anomalie à corriger, mais comme un fait social total, structurant les

relations au savoir, les hiérarchies symboliques et les conditions de légitimation dans les mondes économiques périphériques.

En somme, penser la cyber-ignorance managériale comme un phénomène ethnographiable, c'est refuser de la réduire à une carence fonctionnelle. C'est reconnaître en elle une forme d'intelligence pratique, une réponse située à l'injonction numérique, une stratégie de survie parfois, un acte de résistance parfois aussi. C'est, enfin, ouvrir une voie pour une sociologie critique du numérique en entreprise, attentive aux voix faibles, aux pratiques ordinaires, et aux rationalités non hégémoniques.

Les références bibliographiques

- AlHogail, A., & Mirza, A. (2021). *Information security ignorance: An exploration of the concept and its implications*. Computers & Security, 105, 102227. https://doi.org/10.1016/j.cose.2021.102227
- Anact. (2023). *Conditions de travail dans les TPE/PME – Revue des conditions de travail*.
- Banque des Territoires. (2020). *Inclusion Numérique des TPE, rapport d'expérimentation et recommandations*.
- Berger-Douce, S. (2018). *Transformation numérique et TPE : entre contraintes et opportunités*. Revue Internationale PME, 31(1), 9–32.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). *Digital business strategy: Toward a next generation of insights*. MIS Quarterly, 37(2), 471–482.
- Bitektine, A., & Haack, P. (2015). *The "macro" and the "micro" of legitimacy: Toward a multilevel theory of the legitimacy process*. Academy of Management Review, 40(1), 49–75.
- Bretag, T. (2016). *Challenges in addressing plagiarism in education*. PLoS Medicine, 13(12), e1002183. https://doi.org/10.1371/journal.pmed.1002183
- Camp, J. L. (2006). *Designing for trust*. In *Trust and Risk in Internet Commerce* (pp. 27–43). Springer.
- Cranor, L. F., Egelman, S., & Sheng, S. (2008). *User interface design for secure systems*. Foundations and Trends® in Human–Computer Interaction, 1(4), 307–402.
- CyberEdu. (n.d.). *Programme pédagogique de sensibilisation à la cybersécurité*. https://www.cyberedu.fr
- Drieets – France Relance. (2021). *Ma TPE a rendez-vous avec le numérique*.
- Érudit. (2024). *Les pratiques de gestion des médias sociaux par les TPE*.
- France Num. (2023). *Baromètre France Num 2023 : la transformation numérique des TPE/PME*. https://www.francenum.gouv.fr
- France Num. (2023). *Baromètre sur la transformation numérique des TPE/PME*. Agence France Numérique.
- Gibson, C. B., & Gibbs, J. L. (2006). *Unpacking the concept of virtuality: The effects of geographic dispersion, electronic dependence, dynamic structure, and national diversity on team innovation*. Administrative Science Quarterly, 51(3), 451–495.
- Grafiati. (2024). *Transformation numérique des TPE – Bibliographie*.
- OECD. (2021). *The Digital Transformation of SMEs*. Organisation for Economic Co-operation and Development. https://doi.org/10.1787/27f4eacb-en
- OCDE. (2021). *Digital Transformation of SMEs: Trends and Challenges*. OECD Publishing. https://doi.org/10.1787/27f4eacb-en
- Schallum, P., & Jaafar, F. (2021). Dans *Médias sociaux : perspectives sur les défis liés à la cybersécurité, la gouvernementalité algorithmique et l'intelligence artificielle*.

- Science & Ignorance (INIST-CNRS). (n.d.). *Études sur l'ignorance dans les sciences et les controverses scientifiques*. https://scienceetignorance.inist.fr/
- SERENE-RISC. (2020). *Cybersecurity awareness and education resources*. https://www.serene-risc.ca
- Suchman, M. C. (1995). *Managing legitimacy: Strategic and institutional approaches*. Academy of Management Review, 20(3), 571–610.
- Zimmerman, M. A., & Zeitz, G. J. (2002). *Beyond survival: Achieving new venture growth by building legitimacy*. Academy of Management Review, 27(3), 414–431.

ANNEXE

Préconisations stratégiques

À la lumière des résultats de cette enquête et des perspectives ouvertes par l'analyse ethnographique, nous proposons trois axes d'action pour les décideurs publics, les institutions d'accompagnement et les chercheurs.

1. Intégrer l'ignorance comme objet d'intervention à part entière

- Abandonner les approches centrées exclusivement sur le « manque de compétences » pour penser l'ignorance comme une stratégie managériale de protection ou de délégation.
- Élaborer des outils de diagnostic qui intègrent les représentations sociales du numérique, les rapports à la légitimité, et les mécanismes de dissimulation.

2. Territorialiser les politiques de digitalisation

- Concevoir des dispositifs d'acculturation numérique contextualisés, prenant en compte les réalités de l'isolement, des logiques gestionnaires rurales et des contraintes identitaires des dirigeants.
- Déployer des intermédiaires numériques de proximité, capables de nouer des relations de confiance, de diagnostiquer sans stigmatiser, et de construire des trajectoires de montée en compétence acceptables socialement.

3. Revaloriser la légitimité numérique comme enjeu identitaire

- Proposer des formations à la fois techniques et narratives, centrées sur le récit professionnel, la valorisation de l'expérience, et l'intégration du numérique dans la trajectoire entrepreneuriale.
- Créer des espaces de pair-à-pair où les dirigeants peuvent partager leurs doutes, expérimenter sans jugement, et reconstruire une légitimité numérique à leur rythme.
- Promouvoir des figures locales inspirantes, des dirigeants de TPE ayant réussi une appropriation progressive et contextualisée du numérique, pour créer des effets d'identification positifs.