

# PECEPHOBIE Peur de l'ordinateur

## Ou Cyberphobie

**Phobie non officielle, non reconnue, non spécifique,  
non classifiée en tant que trouble anxieux défini dans le DSM-5 et la CIM-11**

Je retiens l'acception psychologique (aversion anxieuse envers l'informatique et les dispositifs numériques), puis ses déplacements sociologique et philosophique.

### Statut nosographique

La cyberphobie n'a pas d'autonomie diagnostique : le DSM-5 ne la retient pas, et elle relèverait au mieux de la phobie spécifique, type « autre », ou d'une anxiété situationnelle. La littérature anglophone parle de *computerphobia* ou de *computer anxiety*. Elle a été opérationnalisée par des instruments psychométriques, notamment la *Computer Anxiety Rating Scale* (Heinssen, Glass & Knight, 1987), puis par les travaux de Rosen et Weil sur la « technophobie », et ceux de Brosnan (1998). Le point méthodologique central est la distinction entre :

- une **phobie** au sens strict (réaction anxieuse disproportionnée, évitement, détresse cliniquement significative) ;
- une **attitude négative** ou un scepticisme technologique, relevant de la psychologie sociale de l'acceptation technologique (modèles TAM, UTAUT), sans pathologisation.

La plupart des mesures saisissent le second registre et lui appliquent abusivement le lexique du premier.

### Étiologie et facteurs modérateurs

Les modèles invoquent la faible auto-efficacité informatique (Bandura), l'expérience antérieure d'échec ou d'humiliation instrumentale, la fracture générationnelle (le « migrant numérique » de Prensky, notion discutée), et des variables de genre largement modulées par la socialisation. L'anxiété porte moins sur l'objet que sur la perte de maîtrise, l'irréversibilité d'une erreur, et l'opacité des systèmes (*boîte noire*).

### Déplacement vers la cybercrainte

Le glissement vers la peur des cybermenaces (fraude, surveillance, exposition des données) relève plutôt de la littérature sur le *fear of crime* (Ferraro) : le sentiment d'insécurité y est dissocié du risque objectif. La cyberphobie devient alors l'effet d'une grammaire médiatique du risque, d'où la thèse d'une panique morale (Cohen) périodiquement reconduite à chaque innovation médiatique.

### Lecture philosophique

Le préfixe renvoie à *kubernêtikê*, l'art du pilotage, via Wiener (1948). Redouter le cybernétique, c'est redouter la délégation du gouvernement à des boucles de rétroaction. L'*Unheimliche* freudien (1919), à partir de Jentsch et de la figure de l'automate, éclaire

l'inquiétante étrangeté des artefacts mimétiques, que prolonge la *vallée de l'étrange* (Mori, 1970). Chez Anders, la « honte prométhéenne » devant la perfection des appareils, chez Ellul l'autonomie du système technicien, chez Heidegger l'arraisonement (*Gestell*), fournissent la version spéculative de ce que la psychométrie traite comme symptôme. La question est alors de savoir si la cyberphobie est un trouble de l'ajustement ou une lucidité critique pathologisée.

### **Trois pistes d'élaboration avec Claude IA**

1. *Une critique épistémologique de la mesure : la psychométrie de l'anxiété informatique produit-elle son objet en confondant résistance rationnelle et phobie ?*
2. *Une généalogie comparée du luddisme, de la technophobie et de la cyberphobie comme catégories de disqualification des résistances technologiques.*
3. *Une lecture psychanalytique de l'opacité algorithmique : l'Unheimliche à l'ère des systèmes d'apprentissage, entre intelligibilité perdue et angoisse de substitution.*

## **LE PECEPHOBE OU CYBERPHOBE**

### **La thèse de la performativité de la mesure**

L'hypothèse selon laquelle la psychométrie produirait son objet relève d'une lecture hackingienne : la catégorisation « fait » des types de personnes (*making up people*, Hacking) en instituant un espace de classification où des sujets viennent se loger, puis se reconnaître. Dans le cas de la *computer anxiety*, l'opération est double. La CARS de Heinssen, Glass et Knight (1987) ne découvre pas un trait préexistant : elle stabilise un construit par agrégation d'items hétérogènes (appréhension, évitement, malaise anticipatoire), puis ce construit, doté d'un nom et d'une échelle, acquiert la consistance d'une entité. Le geste est celui que Danziger a décrit pour la psychologie en général : l'instrument constitue l'objet qu'il prétend enregistrer.

### **Les défauts de validité de construit**

Trois lignes de fragilité se dégagent.

**a) Indistinction sémantique des items.** Les énoncés de type « je crains de détériorer l'ordinateur » ou « les machines me mettent mal à l'aise » ne discriminent pas entre une peur affective, une estimation probabiliste d'un coût (perte de données, irréversibilité) et un jugement normatif. L'échelle de Likert agrège ces registres en un score unidimensionnel, alors que leur statut logique diffère : l'un est un état, l'autre une évaluation, le troisième une position.

**b) Absence de critère externe.** Le DSM exige une détresse cliniquement significative, une disproportion et un évitement persistant. La plupart des études sur échantillons étudiants ou professionnels n'établissent aucun seuil clinique ; elles corrélaient des scores continus avec des variables d'usage. La validité convergente est donc circulaire : l'anxiété est « validée » par sa

corrélation avec la moindre utilisation, laquelle est précisément ce que l'anxiété était censée expliquer.

c) **Normativité implicite du critère d'adaptation.** Le score élevé est traité comme un déficit à réduire, de sorte que la variable dépendante est l'adoption. Le dispositif épistémique est tacitement prescriptif : la résistance devient un obstacle à l'implantation, non une donnée cognitive. L'héritage du TAM (Davis, 1989) et de l'UTAUT consolide ce biais pro-innovation, que Rogers désignait déjà comme *pro-innovation bias* dans la diffusion des innovations.

### **Résistance rationnelle : de quoi parle-t-on ?**

La distinction exige un critère. On peut retenir, en première approche, qu'une résistance est rationnelle lorsqu'elle est (i) **indexée à des raisons** que le sujet peut expliciter, (ii) **sensible à l'information** (révisable sous l'effet de preuves ou de dispositifs de réassurance), (iii) **proportionnée** à un risque ou à un coût identifiable. La phobie se définit inversement par son insensibilité à la contre-évidence et sa disproportion. Or ces critères ne sont pas mobilisés par les instruments, qui mesurent l'intensité sans interroger la structure inférentielle de la réponse.

Le problème est que ce critère n'est lui-même pas neutre. Dès les travaux de Zuboff (1988) sur l'automatisation du travail de bureau, l'anxiété des opérateurs est lisible comme une réponse rationnelle à la dépossession des savoir-faire tacites et à l'intensification de la surveillance. La résistance exprime alors un calcul sur la répartition du pouvoir plutôt qu'un affect irrationnel. De même, les analyses de Noble sur les machines-outils à commande numérique, ou la sociologie de la traduction autour de l'appropriation des outils, mettent en évidence que le « refus » est souvent une négociation de l'usage.

### **Le point de rupture : la causalité inverse et l'asymétrie d'expertise**

Brosnan (1998) comme Bandura insistent sur l'auto-efficacité, ce qui déplace l'explication vers le sujet. Mais la littérature en *human-computer interaction* (Norman, *The Design of Everyday Things*) renverse la perspective : l'anxiété peut résulter d'une **opacité de conception** (absence de *feedback*, de réversibilité, de modèle conceptuel visible). Le « phobique » détecte alors correctement une propriété du système, à savoir son hostilité à l'erreur. Le diagnostic individualise ce qui relève d'un défaut de l'artefact. C'est un cas de ce que Latour nommerait un transfert de responsabilité du dispositif vers l'utilisateur, rabattu sur le registre psychique.

### **Ce que n'établit pas l'argument**

Il serait imprudent de conclure à la pure fabrication. Des états anxieux disproportionnés existent et sont cliniquement documentés ; le réalisme minimal sur le phénomène reste défendable (au sens d'un « réalisme interactif » de Hacking, où le construit boucle sur ses sujets sans être illusoire). La critique porte sur la **jonction** : l'échelle continue d'« anxiété » ne

permet pas de séparer les populations, de sorte que ni la thèse d'un réel phobique massif, ni celle d'une pure construction ne sont testables avec ces outils. Une stratégie recevable serait **mixte** : analyse en classes latentes pour identifier d'éventuels profils distincts, entretiens d'explicitation des raisons, manipulation expérimentale de la réversibilité ou de la transparence du système pour tester la sensibilité à l'information.

### ***Trois directions d'élaboration avec Claude IA***

1. *Une reconstruction formelle du critère de rationalité de la résistance (sensibilité à l'information, indexation à des raisons, proportionnalité), confrontée aux conceptions de la rationalité limitée et à la psychologie du risque (Kahneman, Slovic), qui brouillent la frontière entre heuristique raisonnable et biais.*
2. *Une analyse du rôle du pro-innovation bias dans l'institutionnalisation des instruments de mesure, à partir d'une sociologie des sciences appliquée au champ des technology acceptance studies.*
3. *Une extension à l'IA générative : la méfiance envers les systèmes opaques y est-elle déjà en voie de pathologisation sous le label d'« anxiété algorithmique », et à quelles conditions pourrait-elle être, au contraire, consacrée comme compétence critique ?*

## **LA PEUR DES CYBERMENACES**

### ***Mobilisation de références théoriques sur la peur numérique.***

#### **Reconfiguration de l'objet**

Le déplacement n'est pas anodin : la peur des cybermenaces ne relève plus d'une psychologie de l'utilisateur face à l'artefact, mais de la sociologie du risque et de la criminologie du sentiment d'insécurité. La littérature sur le *fear of crime* (Warr, Ferraro) distingue la **perception du risque** (composante cognitive, estimation d'une probabilité de victimation) de la **peur** proprement dite (composante affective). Appliquée au cyberspace, cette distinction se heurte à une difficulté propre : la victimation y est fréquemment non perçue, différée ou non attribuable (compromission silencieuse de données, fraude détectée a posteriori), si bien que l'expérience individuelle ne fournit qu'un ancrage lacunaire à l'estimation du risque.

#### **Le renversement du critère de proportionnalité**

Dans la critique précédente, la disproportion de l'anxiété à un risque objectif servait de critère discriminant entre phobie et résistance rationnelle. Ici, ce critère devient quasi inopérant : il n'existe pas d'étalon stable du « risque objectif » cybernétique. Le *dark figure* de la cybercriminalité, la sous-déclaration, l'hétérogénéité des taxonomies (Wall) et le caractère contesté des estimations de coût (Anderson et al., 2013, sur la mesure du coût de la cybercriminalité) interdisent de trancher entre surestimation et sous-estimation. Il s'ensuit une inversion possible de la thèse du *fear of crime* classique, où la peur excède le risque : on

peut soutenir que la crainte, dans certains segments, est **inférieure** à l'exposition réelle, ce qu'attesterait la persistance de pratiques de sécurité défailantes (réutilisation de mots de passe, absence de mises à jour).

### **Les résultats empiriques et leurs limites**

Les travaux sur la peur de la cybercriminalité en contexte européen (Virtanen, 2017) et sur la peur de la fraude financière en ligne (Brands & van Wilsem) reproduisent partiellement le patron du *fear of crime* : effet de la victimation antérieure, rôle des vulnérabilités perçues, effet médiateur des comportements en ligne. Mais la corrélation entre peur et victimation reste faible et instable, ce qui rapproche le terrain du « paradoxe de la victimation » classique, tout en exigeant prudence : la causalité est vraisemblablement bidirectionnelle, la peur modifiant l'exposition (éviter, vigilance), laquelle modifie à son tour le risque réel. Les devis transversaux dominants ne permettent pas de démêler cette boucle.

### **L'économie politique de la menace**

Trois mécanismes de production sociale de la peur méritent distinction.

a) **Sécuritisation.** Dans le cadre de l'École de Copenhague, Hansen et Nissenbaum (2009) montrent que le « cyber » est constitué en objet de sécurité par des actes de langage faisant intervenir des scénarios hypothétiques (le « Pearl Harbor numérique », selon la rhétorique de Panetta en 2012), que Lawson (2013) analyse comme des récits de *cyber-doom* à faible ancrage factuel, et que Rid (2012) critique en contestant la pertinence même de la catégorie de cyberguerre.

b) **Asymétrie d'information sur le marché de la sécurité.** Anderson et Schneier ont décrit la sécurité comme un bien dont la qualité est inobservable pour l'acheteur, d'où une dynamique de type *market for lemons* et un recours au « théâtre de sécurité », où le dispositif rassure sans nécessairement protéger. Les prescripteurs commerciaux ont un intérêt structurel à entretenir un niveau de crainte soutenant la demande.

c) **Société du risque et peur liquide.** Chez Beck, le risque numérique illustre le risque réflexif produit par la modernité elle-même ; chez Bauman, la peur diffuse, sans objet localisable, se distingue de la peur d'un danger identifié. La menace cybernétique, ubiquitaire et invisible, réalise presque idéalement cette seconde forme.

### **Le paradoxe des appels à la peur.**

L'hypothèse intuitive selon laquelle l'accroissement de la crainte renforcerait la protection est infirmée par les modèles de motivation à la protection (Rogers, 1975) et le modèle étendu des processus parallèles (Witte, 1992) : lorsque l'efficacité perçue de la réponse est faible, l'appel à la peur induit un **contrôle de la peur** (dénier, évitement défensif) plutôt qu'un **contrôle du danger**. Les observations sur la *security fatigue* (Stanton et al., NIST, 2016) et sur l'échec des

campagnes de sensibilisation (Bada, Sasse & Nurse, 2019) convergent. Le paradoxe de la vie privée (Barnes, 2006 ; Acquisti), c'est-à-dire la dissociation entre préoccupation déclarée et comportement, relève sans doute moins d'une irrationalité que d'un calcul d'impuissance face à des asymétries de pouvoir : on retrouve la structure de la résistance rationnelle précédemment discutée, mais déplacée vers la résignation (*privacy resignation*, Draper & Turow).

### **Conséquence épistémologique.**

La mesure de la peur des cybermenaces affronte donc un problème de **référence** (quel risque objectif ?) plus radical que celui de l'anxiété informatique. Le sentiment d'insécurité y devient un indicateur à double lecture : symptôme d'une exposition réelle sous-perçue ou effet d'un discours de menace. Tant qu'aucune mesure indépendante de l'exposition n'est disponible, les deux lectures restent empiriquement sous-déterminées.

### **Trois directions d'élaboration avec Claude IA**

1. *Une analyse comparée de la validité des instruments de mesure de la peur de la cybercriminalité, en discutant spécifiquement l'absence d'étalon du risque objectif et les possibilités de triangulation (données de victimation déclarée, journaux techniques, audits de pratiques).*
2. *Une généalogie discursive du « cyber-doom » en tant que dispositif de sécuritisation, articulée à l'économie de l'industrie de la cybersécurité et à ses incitations à l'amplification.*
3. *Une confrontation entre la thèse de la résignation (privacy resignation) et celle de la résistance rationnelle : la passivité face aux cybermenaces est-elle un déficit de motivation protectrice ou la reconnaissance lucide d'une asymétrie structurelle, au sens où le coût individuel de protection excède le bénéfice attendu ?*