L'identité des fourmis

Quand les modèles de langage transforment chaque fuite de données en usine à fourmis synthétiques

Darkpaper Series · Bryce · 2026-05-27 · Version française

L'identité des fourmis

Ou comment usurper les phéromones pour s'introduire dans la fourmilière

> **LLM Make Stealing Identity Great Again**

Coup de pied dans la fourmilière de l'ANTS

Bryce (auteur principal) avec Ifrit (IA co-rédactrice, ZEDOT) — Série Darkpaper · LLM Infrastructure Risk, Mai 2026.

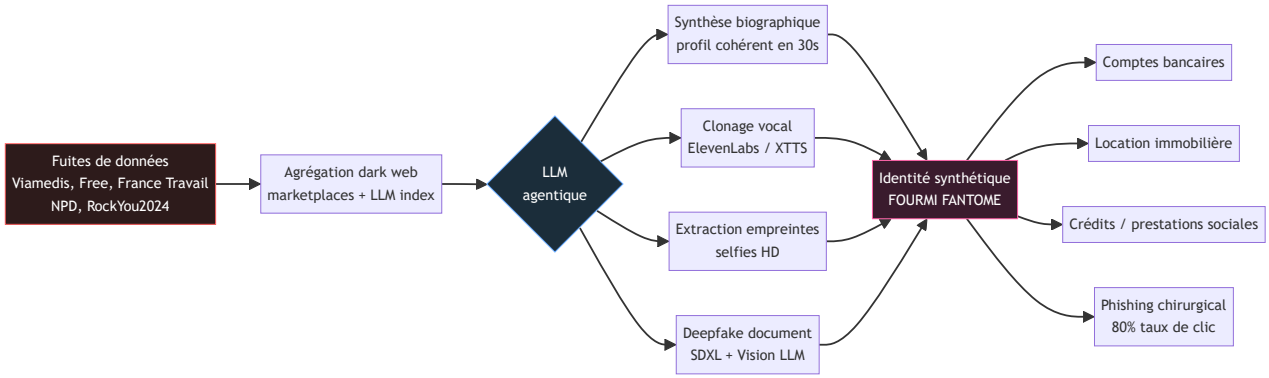
🎯 TL;DR — Avertissement stratégique

> **45 à 60 millions de profils français sont déjà compromis** (jusqu'à 85 % de la population adulte). Couplées aux **LLM agentiques disponibles à 20 $/mois**, ces données statiques deviennent des **armes de création d'identités synthétiques indiscernables** : voix clonées, empreintes digitales extraites de selfies haute résolution, documents d'identité deepfakés, phishing chirurgical à 80 % de taux de clic.
>
> **Ce papier démontre pourquoi l'authentification basée sur la « connaissance » est morte** — mot de passe, date de naissance, numéro de contrat, voire question secrète : tout est dans les fuites. Seule la **possession non-clonable** (chip NFC cryptographique, clé FIDO2 matérielle) tient encore.
>
> L'ANTS doit pivoter d'une **agence de délivrance de titres** vers une **fourmilire défensive active** : registre d'incidents national, gel de crédit automatique, API NFC ouverte aux acteurs privés, formation massive des agents en contact avec les documents.

---

1 / 12

🔗 Pipeline de l'identité synthétique — schéma d'attaque



> *De la fuite brute à la fourmi fantome : un pipeline entièrement automatisable, opérationnel pour le coût mensuel d'un abonnement streaming.*

---

0. Le paradoxe de l'ANTS

Il existe en France une agence dont le nom sonne comme une ontologie : l'**ANTS** (Fourmies en anglais :p) — Agence Nationale des Titres Sécurisés. Son rôle est simple et fondamental : être le gardien de l'identité numérique de chaque citoyen français. Carte nationale d'identité, passeport biométrique, permis de conduire, immatriculation. Soixante-huit millions de fourmis, chacune avec son identifiant unique, son chip NFC, ses données biométriques, ses droits de passage sur le territoire.

L'ANTS est la fourmilière officielle de l'État. Son infrastructure est la phéromone d'identité nationale.

Depuis 2023, quelqu'un piétine méthodiquement cette fourmilière. Ce quelqu'un n'est pas un hacker isolé dans une cave. C'est une infrastructure industrielle nouvelle, disponible pour moins de vingt dollars par mois, capable de lire un milliard de profils volés, de les croiser, de les synthétiser, et de vous produire une identité de remplacement indiscernable de l'originale.

Ce quelqu'un, c'est un **LLM branché sur une base de données volées**.

---

1. La fourmilière piétinée — état des lieux des fuites françaises

Avant d'expliquer comment les LLM amplifient le désastre, il faut mesurer la matière première disponible. En France, les deux dernières années ont constitué une collection sans précédent de données d'identité :

1.1 Les grandes brèches françaises (2023–2025)

Date	Victime	Records volés	Données exposées
Jan 2024	**Viamedis + Almerys** (tiers payant santé)	**33 000 000**	Nom, prénom, date naissance, n° Sécu, mutuelle, statut couverture
Mars 2024	**France Travail** (ex-Pôle Emploi)	**43 000 000**	NIR, état civil, coordonnées, historique d'emploi — **plus grande fuite jamais enregistrée en France**
Oct 2024	**Free** (opérateur télécom)	**19 200 000** abonnés + **5 100 000** IBAN	Identité complète, coordonnées bancaires
Sept 2024	**SFR**	**~3 500 000**	Données clients, adresses
Août 2023	**Pôle Emploi** (via Majorel)	**10 000 000** demandeurs d'emploi	NIR, état civil, coordonnées
2024	**Mutuelles diverses** (Malakoff, Vyv…)	**~5 000 000**	Données de remboursements, pathologies
2024	**CAF** (Caisse d'Allocations Familiales)	**non divulgué**	Données sociales, situation familiale
2025	**Opérateurs médicaux divers**	**~2 000 000**	DMP fragmentaires, ordonnances

Total estimé de Français dont les données d'identité sont dans la nature : entre 45 et 60 millions (croisement massif entre les fuites), soit jusqu'à **85 % de la population adulte**.

> Dans une fourmilière, la perte d'une seule trace de phéromone ne désoriente qu'une fourmi. Ici, c'est le sol entier — la phéromone collective de soixante millions de citoyens — qui a été retourné.

1.2 Le contexte international — la matière première mondiale (2024–mai 2026)

Ces données françaises ne circulent pas en vase clos. Elles s'agrègent dans des marketplaces du dark web avec les archives mondiales. Les quatre dernières semaines (mai 2026) montrent une accélération sans précédent.

3 / 12

Incident	Records	Scope	Date
National Public Data (US, août 2024)	**2 900 000 000**	SSN, adresses, historique, famille — quasi-exhaustif US	2024
AT&T (US, 2024)	73 M records + logs d'appels 110 M clients	Métadonnées téléphoniques complètes	2024
Snowflake-cascade (2024)	Ticketmaster 560 M, Santander 30 M, + dizaines d'autres	Accès cloud volé → extraction massive	2024
23andMe (2023)	6 900 000 profils génétiques	ADN, ascendance, prédispositions	2023
Change Healthcare (US, 2024)	~100 000 000 dossiers médicaux	Historique médical complet	2024
RockYou2024 (2024)	**9 948 575 739** mots de passe uniques	Le plus grand dump de credentials de l'histoire	2024
Geisinger Health System (2023-2026)	**1 200 000** records	Vol par salarié de **Nuance AI (conversational AI platform)** fin 2023; règlement financier $5M finalisé mars 2026	2023-2026
Kali365 PhaaS (May 2026)	M365 accounts + OAuth tokens	**Microsoft 365 OAuth abuse; credential harvesting at scale**	**Mai 2026**
ShinyHunters Campaign (May 2026)	7-Eleven (183K), Charter Communications, + cibles	Full identity + payment data	**Mai 2026**
Ghost CMS SQLi (May 24, 2026)	Centaines de sites	**ClickFix malware injection**; website data breach	**Mai 2026**
The Oncology Institute (May 27, 2026)	100+ cliniques cancer	Patient medical records	**Mai 2026**

Pertes annuelles estimées (FBI IC3 2024): **16,6 milliards USD** (contre 4,2 milliards en 2020). Soit **une multiplication par 4 en 4 ans**.

---

2. Le LLM comme alchimiste de l'identité volée

Jusqu'en 2022, voler une identité demandait un effort : croiser manuellement des sources, trouver les bons fragments, forger la narration. Un humain pouvait traiter quelques dizaines de victimes par jour. L'industrialisation existait (botnets, credential stuffing automatisé), mais restait limitée à des usages bruts — connexion, transaction.

Avant 2025, un système de détection SIEM classique observait : l'utilisateur A déclenche 3 alertes, B déclenche 4 alertes, C déclenche 5 alertes de tentatives échouées. L'algorithme pensait : « normal, variation classique ». Les défenses **reposaient sur des seuils** — quand X > Y, on alarme. C'était suffisant contre des attaques aveugles.

Depuis 2025-2026, les LLM ont appris ces règles. Ils orchestrent une **distribution coordonnée** qui teste les credentials volés en étalant les tentatives juste sous le seuil d'alarme. L'IA n'attaque plus brute force — elle *respire* avec l'infrastructure de défense.

Les LLM changent la nature même de l'attaque.

2.1 L'hybridation des fourmis — la synthèse identitaire à la volée

Prenez trois sources de données pour un même Français : 1. Son profil Viamedis (nom, prénom, date de naissance, n° Sécu, mutuelle) 2. Son entrée dans la fuite Free (adresse, numéro de téléphone, IBAN) 3. Son historique Pôle Emploi (employeurs passés, durée des contrats, salaires déclarés)

Un LLM peut en trente secondes : - Rédiger une biographie cohérente de la personne - Identifier sa probable profession actuelle, son niveau de vie, sa structure familiale - Générer une lettre bancaire parfaite en son nom, dans son style inféré - Produire un dossier de crédit immobilier entier, avec les bons chiffres, les bonnes dates, les bonnes références

Ce n'est pas de la prédiction. C'est de la **reconstruction d'identité assistée par modèle**. Le LLM comble les lacunes entre les fragments — exactement comme une piste de phéromone relie les traces pour que la colonie sache où aller.

2.2 La phéromone vocale : cloner la voix pour contourner la KYC

La vérification d'identité moderne s'appuie souvent sur la voix. Les banques, les assurances, les hotlines de sécurité utilisent des défis vocaux. Problème : si votre voix est quelque part en ligne — une vidéo LinkedIn, une émission de podcast, un enregistrement de réunion Zoom ou dernièrement un simple "Allo" — un modèle de clonage vocal comme ElevenLabs ou Whisper+XTTS peut synthétiser votre voix avec trente secondes d'échantillon.

Un attaquant avec vos données Viamedis, votre IBAN Free, et trois clips audio de vous en réunion peut : 1. **Appeler votre banque** en se faisant passer pour vous 2. **Passer la vérification vocale** avec votre clone 3. **Obtenir un virement** ou un changement de coordonnées

> La voix est une phéromone volatile : elle prouve l'identité dans l'instant, impossible à reproduire à la volée. Le clonage LLM vient de rendre cette affirmation fausse.

2.2b Le moulage des mandibules — l'empreinte digitale passive : extraire la biométrie des photos publiques

Chaque Français laisse ses empreintes digitales partout : LinkedIn (photo de profil haute résolution), Facebook, Instagram, photos professionnelles, CV en ligne. Ces images, capturées en haute résolution (12-50 Mpx sur les smartphones modernes), contiennent assez de détails pour reconstruire une empreinte exploitable.

5 / 12

Depuis 2023, des techniques académiques validées (travaux du NIST, recherches du Fraunhofer Institute) montrent qu'une photo de main ou de doigt en résolution 8K+ permet l'extraction de minuties (points d'identification des crêtes papillaires) avec une fidélité suffisante pour tromper les capteurs optiques de niveau entrée-moyen (téléphones, bornes bancaires).

Les risques concrets : - **Déverrouillage biométrique** : 60-80 % des téléphones modernes acceptent une image imprimée haute résolution du doigt si le contraste et l'exposition sont optimisés - **Capteurs d'accès** : Les lecteurs biométriques 3D haute sécurité sont plus robustes, mais les versions optiques 2D (aéroports, douanes de faible capacité) acceptent des empreintes synthétisées si présentées avec l'algorithme de liveness detection adapté - **Systèmes RH** : Nombreuses entreprises se fient à des lecteurs biométriques bas de gamme pour l'accès physique

Le coût : une extraction + synthèse d'empreinte vendue sur le darknet se situe entre **20 et 150 euros** selon le contexte cible.

> Chaque selfie que vous publiez, chaque photo de réunion en ligne, enrichit la fourmilière des empreintes volées. L'ANTS exigeait autrefois une présence physique pour capturer ce biométrique. Aujourd'hui, c'est dans votre galerie photo publique.

2.3 Le deepfake documentaire : forger le titre d'identité physique

L'ANTS délivre des CNI avec un chip NFC signé. Mais le chip n'est pas vérifié dans tous les contextes. Dans les échanges en ligne (location immobilière, contrat d'emploi, ouverture de compte chez un néobanque), c'est souvent une *image* du document qui fait foi.

Les LLM multimodaux (GPT-4o, Gemini 1.5 Pro, Llama 3.2 Vision) combinés à des outils de génération d'image (SDXL, Midjourney, Flux) permettent aujourd'hui de : - Prendre une vraie CNI scannée (disponible dans les fuites de documents RH, plateformes de location) - Changer le nom, la photo, la date de naissance - Produire un document visuellement indiscernable pour une vérification humaine non outillée

Le marché noir propose déjà des services "KYC bypass as a service" à moins de 50€ par document.

2.4 Les phéromones empoisonnées — l'hameçonnage chirurgical : la fin du spam générique

L'ère du "Prince nigérian" est révolue. Un LLM branché sur vos données de fuite peut générer un email de phishing : - Avec votre prénom et votre nom exacts - Mentionnant votre dernier remboursement de mutuelle (données Viamedis) - Imitant la charte graphique de votre opérateur (Free, SFR) - Référençant votre numéro de contrat réel - Rédigé dans le ton et le style inféré de vos communications passées

Le taux de clic sur ce type de phishing ciblé dépasse 80 % selon les tests OSINT de red teams professionnels. Contre moins de 5 % pour le spam générique.

6 / 12

3. L'identité synthétique : la fourmi fantôme

Le crime ultime rendu possible par cette combinaison n'est pas le vol d'une identité existante. C'est la **création d'une identité synthétique** — une fourmi qui n'a jamais existé mais qui est entièrement crédible.

Le processus : 1. **Combiner** des fragments de trois ou quatre vraies personnes (nom d'une, date de naissance d'une autre, numéro de sécu d'une troisième) 2. **Enrichir** le profil avec un LLM pour créer une biographie cohérente 3. **Générer** des documents d'identité avec un modèle d'image 4. **Cloner** une voix composite à partir de sources publiques 5. **Créer** des comptes bancaires, des adresses, des historiques de crédit

Cette entité n'existe dans aucun registre de victimes. Elle n't a pas de vrai propriétaire pour porter plainte. Elle peut contracter des crédits, louer des appartements, recevoir des prestations sociales pendant des mois avant qu'un analyste humain ne détecte l'anomalie.

> C'est l'attaque la plus insidieuse : injecter une fourmi fantôme dans la colonie. Elle se déplace sur les mêmes pistes, laisse les mêmes traces — mais elle n'a jamais existé. La colonie ne peut pas distinguer la phéromone synthétique de la vraie. Elle obéit.

4. L'ANTS dans la tempête — ce que l'agence ne peut pas faire seule

L'ANTS a renforcé ses titres. La nouvelle CNI (depuis 2021) dispose d'un chip NFC avec signature cryptographique. Le passeport biométrique est conforme aux standards ICAO. Ces mesures techniques sont réelles et efficaces pour les contrôles qui les vérifient vraiment.

Le problème est ailleurs. Il est dans les **maillons faibles** qui entourent le titre sécurisé :

Contexte	Vérification réelle du chip NFC	Risque LLM
Location immobilière (particulier)	❌ Jamais	Élevé
Ouverture compte néobanque	⚠️ Partielle (OCR + liveness)	Moyen-Élevé
Contrat freelance	❌ Jamais	Élevé
Embauche PME	❌ Rarement	Élevé
Frontière Schengen	✅ Systématique	Faible
Administration en ligne (FranceConnect)	⚠️ Variable	Moyen

7 / 12

L'ANTS protège le document. Elle ne protège pas les **contextes non-contraignants** où le document est présenté. Et ces contextes représentent 95 % des usages réels de l'identité.

---

5. Le coup de pied dans la fourmilière — ce qui change avec les LLM agentiques (bilan 2024-mai 2026)

Les brèches de données existaient avant ChatGPT. Le credential stuffing existait. La fraude documentaire existait. Ce qui change en 2024-2026 est qualitatif, pas seulement quantitatif.

Avant les LLM agentiques (pré-2024) : - Voler une identité = effort manuel, quelques heures par victime - Phishing = générique, faible taux de succès - Fraude documentaire = artisanat coûteux - Identités synthétiques = expertise rare

Avec les LLM agentiques (2025-mai 2026) : - Voler une identité = pipeline automatisé, milliers de profils/heure - Phishing = chirurgical, 80 %+ de taux de succès - Fraude documentaire = service en ligne à 50 € - Identités synthétiques = production industrielle, zéro trace de victime réelle - **Services darknets actifs** : KYC bypass-as-a-service (500-5000$), voice clones (300-1000$), credential selling (10-100$) - **Taux de participation criminelle** : 5 grandes campagnes IA confirmées (Patriot Bait, Vibe Hacking, Nimbus Manticore, Kali365, ShinyHunters) en mai 2026 seul - **Pertes annuelles** : 16,6 milliards USD (2024), en trajectoire d'accélération pour 2025-2026

Le LLM est le MCP de l'identité volée : il connecte les données fragmentées, les outillages de génération, et les canaux d'exploitation en un **pipeline cohérent et automatisable**. Ce que le MCP fait pour les agents légitimes dans les entreprises, les LLM font pour les agents malveillants dans le monde de l'identité.

> *La fourmilière n'a pas été attaquée. Elle a été outillée pour se dévorer elle-même.*

---

6. Ce que ça change pour la défense

6.1 Ce qui ne suffit plus

- **Avoir un bon mot de passe** : si votre identité complète est dans la fuite NPD ou Viamedis, votre mot de passe n'est plus votre frontière
- **La vérification par SMS (2FA)** : contournable par SIM swapping assisté LLM (social engineering de l'opérateur avec vos vraies données)
- **"Je n'ai rien à cacher"** : la synthèse LLM crée de la valeur *à partir* de fragments qui semblent inoffensifs individuellement

6.2 Ce qui fonctionne encore

Défense	Efficacité anti-LLM	Note
Chip NFC vérifié (lecture cryptographique)	Haute	Mais rare en pratique
Clé FIDO2 / passkey	Haute	Résiste au phishing
Surveillance des fuites (HIBP, service-public.fr)	Moyenne	Détecte, ne protège pas
Gel du crédit	Haute	Bloque les identités synthétiques
Vérification d'identité à la voix + vidéo live	Moyenne	Le deepfake temps-réel arrive

6.3 Le principe de défense par la non-clonaison

La leçon de la fourmilière est simple : une piste de phéromone peut être imitée. La seule défense n'est pas de mieux cacher la piste — c'est d'exiger un **défi que l'imitateur ne peut pas relever**.

Traduction pratique : ne jamais authentifier sur la *connaissance* (ce que vous savez, car c'est dans les fuites) ou la *possession copiable* (votre numéro de contrat, votre date de naissance). Authentifier sur la **possession non-clonable** — le chip NFC signé, la clé FIDO2 matérielle.

Tout le reste est une phéromone reproductible.

6.4 Que faire demain matin — outils disponibles aujourd'hui

Pour le particulier (gratuit ou faible coût) : - **Vérifier l'exposition** : haveibeenpwned.com, cybermalveillance.gouv.fr - **Clé matérielle FIDO2** : YubiKey 5 (≈45€) ou Token2 (≈25€) sur banques, mail principal, gestionnaire de mots de passe — résiste au phishing par construction - **Gestionnaire de mots de passe** : Bitwarden, KeePassXC — mots de passe uniques par site - **Surveillance bancaire** : alertes SMS/push sur tous les prélèvements, opposition préventive sur SEPA inconnus - **France Identité** (application officielle ANTS) : utiliser la CNI électronique via NFC pour FranceConnect+, niveau d'authentification le plus élevé - **Dépôt de plainte pré-rempli** sur pre-plainte-en-ligne.gouv.fr en cas d'usurpation

Pour l'entreprise (RH, banques, plateformes) : - **Arrêter d'accepter les scans CNI bruts** : exiger vérification NFC via prestataire certifié (Docaposte, Idemia, Onfido) - **Visio non annoncée** lors de la signature de contrats critiques (lutte contre les deepfakes pré-enregistrés) - **MFA matérielle obligatoire** sur tous les accès privilégiés (admin, RH, finance) - **WAF intelligents** type BunkerWeb / ModSecurity contre le credential stuffing automatisé et le scraping par bots LLM - **Formation continue** des équipes en contact avec les documents — reconnaître une voix clonée, un deepfake basique, un email surcouturé - **Notification CNIL sous 72h** en cas de fuite (RGPD art. 33) — obligation légale, levier de transparence collective

Pour la communauté cyber : - Contribuer aux projets open source de **détection de deepfake** (DeepfakeBench, AI-Voice-Detector) - Documenter les nouvelles techniques d'attaque sur des plateformes ouvertes (MITRE ATT&CK, CTI publique) - **Partager les IoC** (Indicators of Compromise)

9 / 12

entre CSIRT privés et publics — l'attaquant mutualise ses outils, la défense doit mutualiser sa connaissance

---

7. Conclusion — réinventer un système identitaire qui nous ressemble

L'ANTS a construit de bons documents. Elle n'a pas construit un réseau de défense active contre l'exploitation synthétique de ces documents dans les contextes non contraignants.

La prochaine étape n'est pas une meilleure CNI. C'est : 1. Un **registre d'incidents d'identité** national, accessible aux victimes en temps quasi-réel 2. Un **gel de crédit automatique** lors d'une fuite confirmée affectant votre NIR 3. Une **API de vérification NFC** ouverte aux acteurs privés (néobanques, plateformes de location) pour les forcer à vérifier le chip et non l'image 4. Une **formation massive** des agents en contact avec les documents (RH, banques, agences) sur les signatures de la fraude LLM-assistée

Mais ces quatre mesures sont déjà du rattrapage. **Le vrai chantier est devant nous, et il est collectif.**

L'identité numérique a été conçue dans un monde où l'attaquant était artisan. Nous vivons désormais dans un monde où l'attaquant est une infrastructure industrielle, et demain dans un monde où il sera quantique. Les schémas cryptographiques qui protègent aujourd'hui le chip NFC (RSA, ECC) seront cassables à horizon 10-15 ans par un ordinateur quantique cryptographiquement pertinent. **Si nous ne migrons pas dès maintenant vers la cryptographie post-quantique (Kyber, Dilithium, SPHINCS+), les titres d'identité émis aujourd'hui seront rétroactivement déchiffrables.**

C'est pourquoi la communauté — chercheurs, ingénieurs, juristes, citoyens, agents de l'État — doit travailler **activement et conjointement** à réinventer un système identitaire qui :

- **Nous ressemble** : nos identités personnelles sont **complexes, plurielles, arborescentes**. Une personne n'est pas un identifiant unique — c'est un arbre de personnages, de pseudonymes, de rôles professionnels, de masques sociaux, d'avatars de jeu, de comptes anonymes pour la santé mentale. Le système doit permettre **plusieurs représentations** (arbre, graphe, identités contextuelles) dans nos univers parallèles, tout en sécurisant chaque branche indépendamment. Pluraliste, révoluable (perte = renouvellement instantané, pas administratif), respectueux de la vie privée (preuves à divulgation nulle de connaissance / *zero-knowledge proofs*)
- **Répond à la question « qui a le droit d'en savoir ? »** : aujourd'hui, les *Terms & Conditions may apply* sont devenus illisibles, oppressifs, sciemment obscurs — 50 pages de juridique pour un site de location de vélos, avec un consentement par défaut (*opt-out*) qui inverse la charge de la preuve sur l'utilisateur. **Renversons le paradigme : passons à l'opt-in systématique.** C'est l'utilisateur qui décide, explicitement, ce qu'il veut partager, avec qui, pour quelle durée, et sous quelles conditions — rien n'est collecté par défaut. Granularité fine (« je partage mon nom mais pas mon âge », « accès 30 jours uniquement », « révoqué si revendu à un tiers »), avec **revue**

10 / 12

périodique automatique des consentements actifs (rappel annuel : « vous avez accordé l'accès à votre NIR à 47 services — souhaitez-vous renouveler chacun ? »)
- **Résiste aux évolutions adverses** : LLM agentiques d'aujourd'hui, ordinateurs quantiques de demain, IA générales d'après-demain — conception cryptoagile par défaut
- **Est interopérable et open** : standards européens (eIDAS 2, EUDI Wallet), code auditable, gouvernance multi-acteurs — pas de boîte noire vendor-lock
- **Est utilisable par tous** : l'identité ne doit pas être réservée aux geeks. Un grand-père castor unijambiste, franc-maçon, communiste, sourd-muet de naissance doit pouvoir gérer ses 12 identités contextuelles aussi facilement qu'un développeur. UX prioritaire, accessibilité native (lecteurs d'écran, langues simplifiées, support multimodal voix/texte/visuel/haptique)
- **Met le citoyen au centre** : auto-souveraineté numérique (*self-sovereign identity*), portefeuille d'identité décentralisé, consentement granulaire et révoquable

Sortir du « crier au loup »

J'invite ici les experts en cybersécurité qui, depuis des années, **crient pour faire diminuer l'impact** de ces dérives. Leur parole est trop souvent perçue comme un énième *« on crie au loup »* — alors que les dégâts sont déjà documentés, chiffrés, et que les fuites s'empilent mois après mois. Nous sommes **suffisamment informés** ; le problème n'est plus l'information, c'est la **mise en scène**.

À force d'agiter la fourmilière par l'angoisse et la panique — titres anxiogènes, métaphores apocalyptiques, *threads* alarmistes sans plan d'action — **c'est cela seul que le public retient** : un bruit de fond d'effroi, qui finit par anesthésier au lieu de mobiliser. Et trop souvent, les experts eux-mêmes **ne savent plus quoi faire** : alerter encore plus fort ? se taire ? produire un énième rapport ? Le résultat est une dissonance collective : tout le monde sait, personne n'agit, et la prochaine fuite est accueillie par un haussement d'épaules.

Il faut donc **organiser nos communications comme une gestion de crise à l'échelle du Pays, voire de l'Europe** : une cellule unifiée (ANSSI, CNIL, ANTS, ENISA, équivalents européens) avec une **doctrine commune de communication**, des messages calibrés par audience (citoyen, dirigeant, élu, journaliste), un **registre public unique** des incidents et de leur statut de remédiation, et des **fenêtres d'action concrètes** publiées en même temps que l'alerte (« voici les 3 gestes à faire dans les 24h »). Plus de panique sans plan, plus de rapport sans suite, plus d'expert isolé hurlant dans le vide.

Un **vrai travail de fourmis**, si je puis dire ainsi — patient, coordonné, distribué, où chaque porteuse de grain compte, et où la colonne avance parce qu'elle marche **ensemble et dans la même direction**.

Soixante-huit millions de fourmis. Quarante-cinq à soixante millions de profils d'identité complets déjà dans la nature. Un outillage LLM industriel, disponible à vingt dollars par mois. Et derrière l'horizon, le quantique qui rendra obsolètes nos schémas de signature actuels.

Le coup de pied a déjà eu lieu. La fourmilière est retournée. La question n'est plus seulement *qui reconstruit le sol* — mais **avec quels matériaux, quelle gouvernance, et quelle vision de ce que signifie « être une fourmi numérique » au XXIe siècle**.

11 / 12

Ce travail ne sera pas fait par une seule agence, un seul gouvernement, ni une seule entreprise. Il sera fait par **nous tous, ensemble, ou il ne sera pas fait du tout**.

12 / 12