PHARE SUR LA RÉSILIENCE NUMÉRIQUE

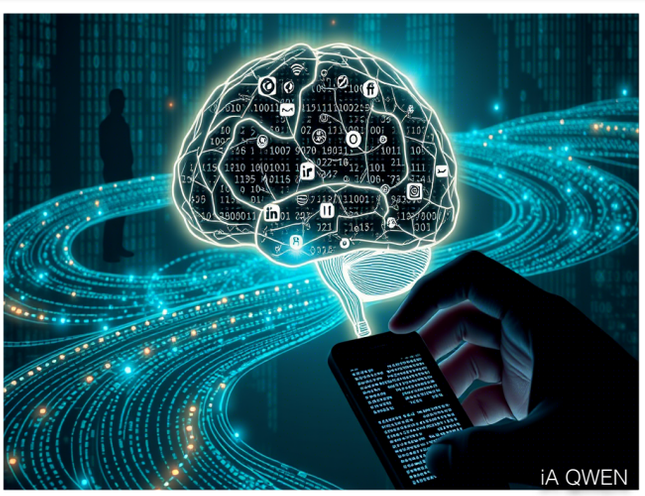
Le XXIè siècle nous a fait entrer dans une ère numérique, "digitale". Aussi passionnante puisse être cette évolution, notamment vis-à-vis du confort que le monde numérique octroie (services rendus, possibilité de conserver et créer du lien avec les gens distants géographiquement, etc.), plusieurs "dangers du numérique" sont bien connus et pointés du doigt :

- Aspects physiques/physiologiques (troubles du fonctionnement cérébral en cas d'utilisation non maîtrisée, notamment sur l'attention, la mémoire, et le développement cognitif).
- Aspect psychologique/santé mentale : dérives des réseaux sociaux avec le cyberharcèlement.
- Manipulations, arnaques, substitut à la vie réelle.
- Vampirisation des données personnelles, et utilisation pour contribuer à la consommation excessive, et la surveillance des populations.

Dans une société où l'outil digital est souvent utilisé pour contrôler les populations, nous sommes nombreux à tendre vers une technophobie, souvent légitime, car on identifie ces nouvelles technologies comme responsables de trop nombreux maux.

Pourtant, et heureusement, il existe plusieurs moyens de se prémunir, voire d'utiliser les outils digitaux/numériques à notre avantage, en tant qu'outils émancipateurs permettant de retrouver notre liberté. De quoi revoir notre manière de percevoir les possibilités qui s'offrent à nous.

Réalisé avec **Icaros**, ce dossier va vous expliquer comment, et vous guider vers votre propre résilience numérique.



Icaros est un ingénieur en télécommunications, dont l'expertise se situe dans la sécurité informatique. Après avoir fondé plusieurs entreprises dans ce domaine, et audité plusieurs dizaines de réseaux, banques et gouvernements, sa prise de conscience en 2008 lors de la "crise financière", face à l'hypnose collective constatée, le pousse à prendre du recul sur ses activités.

Depuis 2020, Icaros met ses connaissances en informatique à disposition de la résistance pour aider des organisations victimes de censure et de surveillance, à mettre en place des solutions alternatives souveraines, libres et ouvertes, afin de s'en affranchir.

Il est également à l'origine du site internet : https://coronacircus.com/

Au travers d'un entretien passionnant (que vous pouvez retrouver sur nos réseaux sociaux, notamment nos chaînes Crowdbunker (https://crowdbunker.com/@lePharandol) et Youtube (https://www.youtube.com/@LesEnfants-Phare), il nous délivre des conseils avisés pour s'intéresser au monde numérique comme outil émancipateur, plutôt que de simplement le boycotter.

I) Enjeux de l'intérêt et la prise en main des outils numériques

Enjeux philosophiques et moraux

Nous faisons le constat d'une tendance volontaire à nous pousser vers du "primitivisme", à savoir la renonciation à la culture, l'innovation et la création. De la même manière, on voit l'alimentation d'une technophobie par l'amalgame que l'innovation et la technologie sont du côté des puissants. Ces derniers sont pourtant incapables de création et d'innovations, et baignent dans l'obscurantisme et les superstitions.

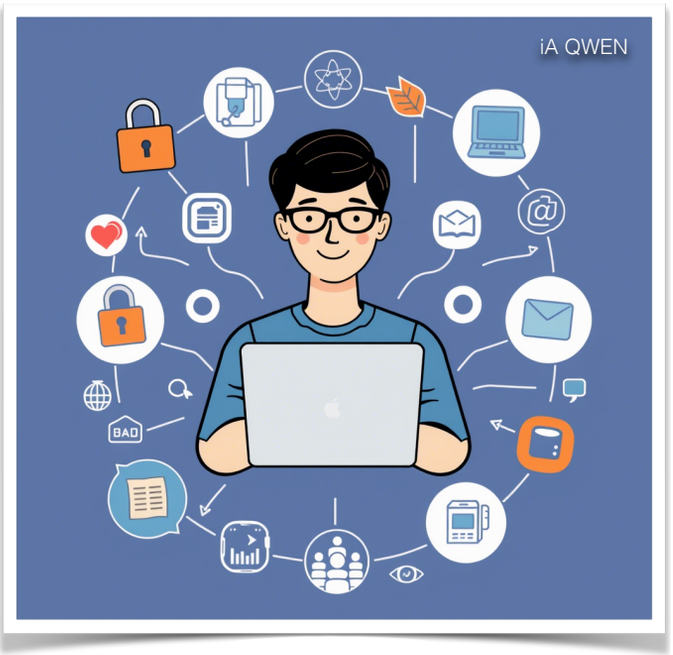
Le peuple est à l'origine des technologies numériques dans une large mesure (même celles reprises par les grosses plateformes qui prétendent à nous surveiller et nous contrôler), de manière décentralisée et unilatérale : la plupart sont fondées sur l'open source, et sont le fruit de la création humaine libre, d'une intelligence collective qui a prouvé sa supériorité.

Renoncer à la technologie, c'est renoncer à l'évolution de la civilisation et à la prospérité dont nous sommes à l'origine, et capables de profiter. C'est une considération morale et philosophique.

Enjeux pratiques

Outre les nombreux bénéfices (innovations) de ces technologies, il y a un constat évident d'une espèce de monopole que s'octroient les puissants pour imposer une sorte de technocratie, en veillant à nous faire croire que les technologies sont trop compliquées pour nous, et nous échappent, et qu'il faut donc soit s'en détacher complètement, soit s'y soumettre. Nous ne sommes plus censés avoir d'opinion à ce sujet, tout comme d'autres (question monétaire, sanitaire, etc.) où l'on nous incite à déléguer notre discernement, notre autorité et notre souveraineté à des pseudo-experts.

Le sujet des technologies numériques – comme celui de la santé – est pourtant tout à fait abordable pour quiconque s'y intéresse.



II) Résilience numérique : par quoi commencer ? Exemples de choses concrètes à mettre en œuvre dans un premier temps

La solution est avant tout comportementale. Il n'y a pas de panacée technique que l'on installe, et tout est réglé. Il est important d'adapter son comportement pour des raisons morales : agir dans le sens du juste et du beau, cela commence par ne pas donner son consentement, ne pas alimenter un système mortifère de nos données, et donc de notre esprit, du fruit de notre créativité et notre imagination.

Nous sommes responsables de ce que l'on fait. Il s'agit d'un petit changement d'habitudes. L'idée n'est pas d'être paranoïaques et de se penser surveillés par la NSA, mais de retirer son consentement à ce système totalitaire et esclavagiste en cessant de profiter des fruits de ce système.

Voici toutefois quelques étapes élémentaires et simples à mettre en place à son échelle.

1) Ne pas partager ses données personnelles, et privées, sur internet.
Si l'information peut paraître évidente pour l'utilisation des réseaux sociaux, elle le semble moins pour des fonctionnalités comme l'iCloud : centralisation des données personnelles (photographies, calendriers, contacts, documents...) sur l'ensemble des appareils Macintosh. Tout est accessible par Apple (et par extension par les autorités étatiques).

Désactiver l'iCloud, c'est certes réduire un peu la flexibilité et l'utilisabilité de l'appareil (facilité de transmission de nos données d'un appareil à un autre), mais c'est gagner en confidentialité de ses données privées, et perdre en traçabilité : on minimise les risques de profils numériques bâtis à notre insu. On gagne également en rapidité d'utilisation de nos appareils.

2) Choisir et protéger ses navigateurs internet
Privilégier Firefox ou Chromium (une version dégooglelisée de Chrome).

Il est possible d'installer 2 extensions à Firefox et Chrome : Privacy Badger (https://privacybadger.org/fr/) ou Ublock-Origin (https://ublockorigin.com/fr).

Privacy Badger

uBlock Origin

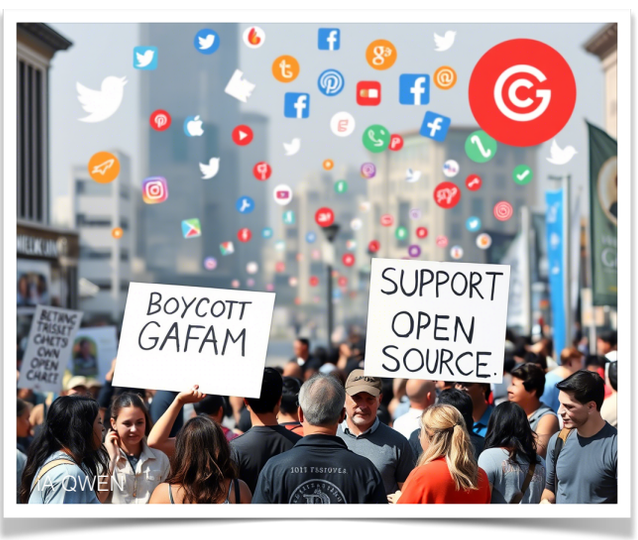
Ces extensions ont un double avantage : éliminer la publicité, et empêcher le "tracking" (cookies, partage des données personnelles, etc.) dans une large mesure.
On peut également utiliser Brave, un navigateur qui contient déjà ces options.

3) Activer le chiffrement du disque dur
Pour les systèmes d'exploitation Windows ou Apple, c'est facile et gratuit à mettre en œuvre, et cela sécurise votre ordinateur et vos données, en rendant contraignant pour tout perquisiteur/pirate intempestif l'accès au contenu de l'ordinateur (si celui-ci est éteint) – ce qui n'est pas le cas d'un simple mot de passe.

Pour le faire, il faut aller dans les paramètres / configuration du système, et chercher "bitlocker drive encryption" sous Windows, et "FileVault" sous Apple, afin d'activer l'encryption du disque.

4) Boycott des GAFAM (et autres grosses plateformes corrompues)
Ces grosses plateformes et entreprises fournissent, sur simple demande des autorités ou de leurs clients publicitaires, toutes nos données personnelles, en plus de les exploiter elles-mêmes.

Le boycott sert avant tout, individuellement, à retirer son consentement (être en accord avec sa conscience individuelle et refuser la domestication), mais il a également l'avantage secondaire, au niveau collectif, d'imposer une contrainte à l'objet du boycott.



La sphère privée individuelle est un droit fondamental. Le but de la civilisation est la transparence des institutions et l'opacité des individus (c'est à dire la sphère privée), et non le contraire.

Il existe de nombreuses alternatives open source, cryptées. Quelques exemples :

- Pour les visioconférences : Jitsi (https://meet.jit.si/), Brave Talk (https://brave.com/fr/talk/) ou bigbluebutton (https://bigbluebutton.org/)…
- Pour le service courriel : Protonmail (https://mail.proton.me/) qui est "Zero knowledge encryption" : on conserve l'initiative de donner l'accès (ou non) à nos correspondances.

On peut remplacer également "Outlook" par Thunderbird (https://www.thunderbird.net/fr/), qui est libre, gratuit et plus sécurisé.

- Pour d'autres services : de nombreuses alternatives aux Google Drive et autres clouds de GAFAM existent, il est possible d'en trouver sur le site Wikilibriste (https://wikilibriste.fr/)

(cf article dans l'édition 26 du Pharandol : Hacker vaillant, rien d'impossible!)

5) Adopter un système d'exploitation libre et opensource

Windows et Apple (MacOs) sont à proprement parler des "malware" : des logiciels malveillants, car espions.

Linux (https://www.linux.org/pages/download/) est au contraire le fruit de l'intelligence distribuée et collective de l'humanité, qui est produit par l'action individuelle unilatétale et libre, et qui rayonne de beauté, de sécurité et de stabilité.

Il existe plusieurs distributions Linux, par exemple Ubuntu (Mint est un peu supérieure), simples d'utilisation et gratuites, qui sont semblables aux logiciels Microsoft, et même compatibles avec ces derniers (exemple : Libre Office qui est compatible avec les formats des Microsoft Office).

Seules limites : utilisation d'applications spécialisées (comme la suite Adobe), ou des jeux vidéos (sauf via Steam), qui ne sont pas toujours adaptés sous Linux.
Pour les entreprises, il existe également des cas particuliers pour l'utilisation de l'open source.

Il faut donc installer ce système d'exploitation en lieu et place de Windows ou Mac.

Une fois que c'est fait, il suffit d'installer Thunderbird comme client mail, un navigateur comme Brave, Firefox ou Chromium (le cas échéant avec les extensions uBlock Origin et Privacy Badger) et la suite bureautique LibreOffice. On profite dès lors du fruit de l'intelligence collective, de l'open source, et on se soustrait à l'emprise des "Big Tech".

L'open source, ou le code en libre accès, signifie que les logiciels sont développés de manière volontaire par des gens partout dans le monde : les compétences de développement peuvent être mises au service du commun (contributionnisme), par un accès libre du code d'un logiciel, et le code développé est intégré au logiciel s'il est validé, par consensus, comme sûr et efficace.

La liberté individuelle produit plus de prospérité, elle fait émerger la beauté et la création unilatérale coopérative, à l'inverse des systèmes pyramidaux et anti-méritocratiques qui sont synonymes de misère. Le principe de l'open source est le principe naturel de la création unilatérale distribuée et volontaire.

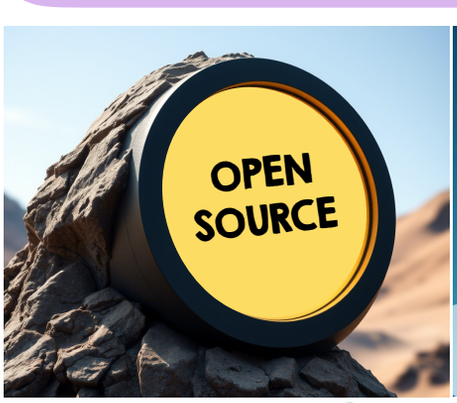
L'open source, fruit de l'intelligence collective, offre le plus souvent une fiabilité et une sécurité supérieures.

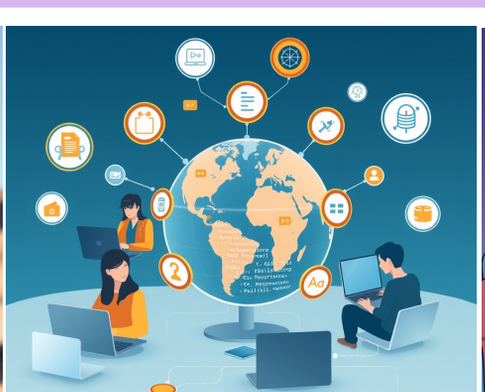
Même chez les "Big Tech", on reconnaît implicitement la supériorité de l'open source, car leurs propres systèmes en dépendent souvent.

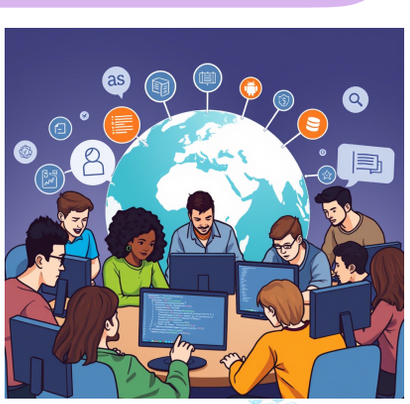
Voici quelques exemples de logiciels performants et spécialisés open source, dont les alternatives commerciales sont onéreuses, qui illustrent bien la puissance de cette intelligence collective : Linux (système d'exploitation https://www.linux.org/pages/download), Godot Engine (logiciel permettant la création de jeux vidéos https://godotengine.org), Blender (logiciel de modélisation, 3D, animations... https://www.blender.org)…

Le logiciel libre et open source, fruit de la contribution volontaire, n'appartient à personne, ou appartient à tout le monde. Le code étant ouvert à tous, chacun peut se l'approprier, et cette concurrence bienveillante permanente pousse à créer du code beau, fiable et efficace, dans le but de l'améliorer en permanence.

Par analogie, si la contribution volontaire était appliquée à l'ensemble de la société, la redistribution des richesses serait vertueuse. On pourrait choisir à quel contrat social on adhère, avec une véritable concurrence institutionnelle, un système politique décentralisé, et une souveraineté individuelle retrouvée.







6) Utiliser des ressources et sources de connaissances libres

Exemple de Libgen (Library Genesis) :

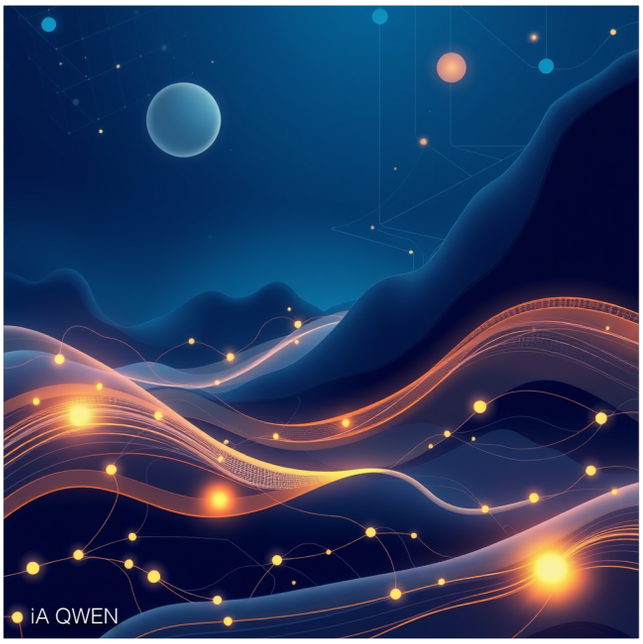
https://libgen.is/ - https://libgen.ac/

LibGen est considérée comme la nouvelle "bibliothèque d'Alexandrie" : 2,5 millions de livres et ouvrages scientifiques y sont en accès libre (NB : le site est censuré en France sous prétexte de défense du copyright, il faut un VPN pour y accéder).

Ce site permet une libre circulation de la connaissance, sans empêcher le soutien (financier) des auteurs par choix des lecteurs/usagers.

Il existe énormément d'autres ressources, mais l'idée phare est de prendre ses responsabilités en la matière : l'intention n'est pas de changer le monde ou de convaincre qui que ce soit, mais d'être des objecteurs de conscience pour éviter d'alimenter un système qu'on ne souhaite pas.

Il n'est pas question de tout réformer en même temps, mais de faire les choses petit à petit à son niveau, participer et contribuer à la prospérité et la beauté dont l'humanité est capable. Au contraire, consommer la "science sans conscience", ou les outils technologiques proposés par des entreprises malveillantes, mène à commettre une faute morale (consentement) et à contribuer à renforcer les chaînes qui maintiennent l'humanité prisonnière.



III) Comment faire si l'on n'a pas les compétences techniques ? Démarche pratique.

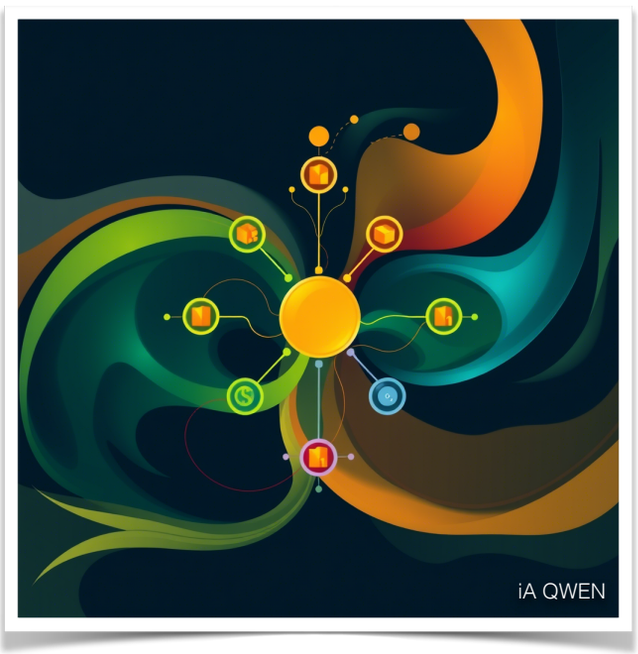
Le premier conseil est de se rendre compte que ce sentiment d'impuissance est inculqué et artificiel : un enfant peut le faire, et par extension, une personne âgée aussi.

Avant même de prendre l'engagement de le faire, il suffit d'aller chercher des tutoriels pour se familiariser voire acquérir des compétences, ou de se rapprocher d'associations ou d'individus qui peuvent aider comme le mouvement des CHATONS : la diversité de talents d'un collectif permet de palier à certaines lacunes individuelles.

Il est aussi possible d'utiliser des outils comme le site wikilibriste (https://wikilibriste.fr) (NDLR : que nous présentons également dans cette édition du Pharandol) pour acquérir des connaissances et se faire guider dans cette démarche.

Le cryptoanarchisme est une philosophie guidée par des principes considérant la technologie numérique comme un outil d'émancipation individuelle, pour peu qu'elle soit libre et ouverte.

Le parallèle de l'open source au niveau politique s'appelle la "panarchie", ou le contrat social volontaire, la décentralisation extrême du pouvoir, et la souveraineté individuelle de droit divin.



IV) Quelles étapes ensuite ?

Tous ces sujets sont congruents. La souveraineté numérique a un lien avec la souveraineté monétaire.

Lorsqu'on poursuit cette évolution personnelle qui consiste à privilégier les solutions libres et ouvertes, on développe naturellement des compétences qui permettent à terme de se défendre non seulement passivement, mais activement aussi. Des projets plus ambitieux sont en construction par des gens qui ont compris ce qui nous attend si on ne fait rien.

Le Mesh Network, ou les Organisations Décentralisées Autonomes (DAO) sont des projets prometteurs pour une émancipation collective du système actuel.
(cf article sur les DAO dans l'édition 26 du Pharandol : Hacker vaillant, rien d'impossible!)

V) Conclusions

Il convient de différencier le hacker du geek.

Le geek (gadget freak) est quelqu'un qui adore les gadgets. Les geeks utilisent la technologie la moins nécessaire, et ce sont ceux qui la comprennent finalement le moins bien.

Le hacker a compris le fonctionnement de la technologie, et sera le dernier à utiliser ces gadgets, le dernier par exemple à déléguer son discernement et ses goûts à l'intelligence artificielle (ou de demander à Alexa d'allumer la lumière). Le vrai développeur qui est familier de la technologie représente l'anti-thèse de la "culture geek".

Un hacker s'oppose naturellement aux monopoles technologiques, aux structures de pouvoir, et aux utilisations liberticides et totalitaires des systèmes d'information (comme l'identité numérique, la vidéosurveillance, les passeports biométriques, etc.).

Être un hacker, c'est développer et exploiter les outils numériques dans un but d'émancipation, en privilégiant l'open source, la cryptographie forte et la décentralisation, et ne pas tomber dans la caricature du "geek" qui s'abreuve de gadgets et d'applications futiles sans les comprendre.

Dossier réalisé par Céline
Avec la participation d'Icaros