- 1) LES GRANDS PRINCIPES DES ASSISTANTS VOCAUX
- 2) ASSISTANTS VOCAUX & CONFIDENTIALITÉ
- 3) AVANTAGES & INCONVÉNIENTS DES ASSISTANTS VIRTUELS
  - a) LE FACTUEL
  - b) LA RÉPONSE STRATÉGIQUE : LE PROXY NATIONAL
- 4) CONFIDENTIALITÉ PAR LE PROXY NATIONAL
  - a) DE NOUVEAUX SERVICES COLLECTIFS
  - b) LES OBJECTIONS AU DÉPLOIEMENT
  - c) LE TIMING POSSIBLE
  - d) LES ENJEUX
- 4) LES RÉPONSES
- 5) LA FORME DE LA RÉPONSE
- 6) LA BASE DE LA RÉPONSE

Alexa fais-ci !
Google fait çà !
Qui n’a pas entendu les publicités multiples et variées des divers assistants vocaux qui sont censés être maintenant des objets aussi indispensables, si ce n’est plus, que nos réfrigérateurs et plaques de cuisson.
En voici un exemple de ce type de publicité.

Tout ceci pour persuader que ce si merveilleux objet se doit d’avoir une présence obligatoire dans chaque foyer de France et de Navarre (et bien sûr dans le monde entier selon Amazon).
Surtout pour demander le temps qu’il va faire (7 secondes de la vidéo) alors que la fenêtre est derrière soi. Passons …

1) LES GRANDS PRINCIPES DES ASSISTANTS VOCAUX

À ce stade, pour ceux qui ne connaissent pas encore le fonctionnement et usage d’un assistant vocal, rappelons juste en quelques mots qu’ils se caractérisent par un boîtier contenant une enceinte sonore et un micro. Le micro est destiné à écouter ce que disent les personnes autour du boîtier afin de comprendre les ordres et demandes qui lui sont adressés. Et restituer par la voie et voix de l’enceinte la

réponse à la demande. (Voir l'explication du fonctionnement sur La Croix)

a) Quelles utilisations ?
Les demandes peuvent tout aussi bien porter sur de la diffusion de musique que des questions d'ordre pratique comme la météo ou sur les dernières nouvelles.

En résumé nous avons donc un haut-parleur qui diffuse des sons et surtout un micro. Un micro qui est en fonctionnement constant toujours en écoute. Et c'est bien là le problème. Car pour que les assistants vocaux puissent vous répondre, ils doivent écouter, constamment, tout le temps, sans arrêt, 24 heures sur 24, 366 jours par an pour les années bissextiles. Cette courte énumération a pour but de faire comprendre à certains que la présence de ce fameux Micro inclut une écoute et donc une surveillance constante.

Certes, il faut dire le nom de l'assistant pour qu'il comprenne qu'on lui parle à lui et pas à une autre personne et qu'il doit donc être prêt à servir. Mais pour ce faire, pour entendre et comprendre qu'on lui parle, l'assistant vocal doit écouter en permanence. En permanence.

2) ASSISTANTS VOCAUX & CONFIDENTIALITÉ

Nous voilà donc avec un **micro**-espion que nous avons, volontairement, placé, en toute ingénuité, à l'intérieur de nos propres murs, au cœur de nos maisons et de nos vies.
Qu'il semble loin le temps du film oscarisé « La vie des autres » [à voir forcément sur Arte, en version originale bien sûr] où, toujours sans vouloir trop divulgâcher, dans l'ancienne Allemagne de l'Est; la si communiste RDA; la principale activité, si ce n'est la seule, du gouvernement (via sa police politique, la STASI) consistait à espionner ces concitoyens en posant des micros dans leurs appartements et maisons.

Voir la bande annonce à 48 secondes pour cette opération de micro.

Maintenant, nous faisons bien mieux. Plus besoin de percer, dévisser, trouer !

Nous plaçons volontairement par nous-mêmes les boîtiers des micros. Aux meilleurs endroits possible.
Nous accueillons à bras ouverts le Cheval de Troie moderne. Celui qui n'envahit pas la Cité.

Celui qui écoute et qui sait tout de nous.

Car qui contrôle l’envoi des phrases captées par ces micros ? Où vont-elles ? Qui les écoute ? Qui les analyse ?
Qui sait vraiment ce qui est envoyé ? Juste nos phrases d’ordres données

Tout ceci est censé être régi par des chartes et des règlements censés protéger nos vies privées, mais dont les principales caractéristiques sont l’élasticité et le trou noir.

> *Bien sûr, il faut modérer cette méfiance en accordant un bénéfice du doute ou de la confiance à la hauteur du respect de la confidentialité et de l'intimité démontrée au quotidien par les entreprises actuelles du monde Numérique, à savoir un indice compris entre le zéro Kelvin et le zéro Fahrenheit.*

Car relater dans le détail et l'exhaustivité des scandales multiples ou bogues ayant déjà eu lieu assécherait les océans d'octets qui sont à notre disposition sur Internet. Voici simplement un lien sur France Info et un autre sur le Figaro.

D'autant plus que maintenant le principe des assistants est étendu à des appareils comprenant des écrans comme ceux du fabricant LENOVO.
Or qui dit écran dit aussi premier pas pour l »intégration de Caméra !

C'est d'ailleurs déjà franchi par Facebook avec son assistant Portal qui en contient bien une ! Officiellement, c'est destiné à des échanges en vidéo. Mais qui décide vraiment de l'ouverture et de la mise en fonction de la caméra ?

Rappelons également que le fondateur de Facebook, Mark Zuckerberg, a solennellement déclaré « qu'il ne souhaitait pas d'une société où il y a une caméra dans le salon de tout le monde« . Ce qui ne l'empêche pas de faire fabriquer des appareils qui en contiennent, car visiblement son salon n'est pas celui de ses clients…

Nous voilà dans un monde encore plus fort que dans les rêves les plus fous des bureaucrates espions de la RDA. Micro et Caméra. Vision et écoute permanente. Ajoutons à ça que ses assistants, si ce n'est déjà fait, vont intégrer d'autres capteurs comme le taux d'humidité, les déplacements d'air, des sensibilités sismiques (une porte qui claque ou qui s'ouvre) etc. et qu'ils vont, en plus, se coupler avec d'autres outils de surveillance. Comme les montres qui peuvent déjà nous donner notre pouls ou notre fréquence cardiaque. Et qui sait bientôt nos flux nerveux ou autres … ?

Nous aurons donc un monde d’espionnage merveilleux et constant où l’on saura tout de nous-mêmes dans la seconde.
Et cela va même encore plus loin.
Par l’analyse, en temps réel, des nos paroles par des experts ou bientôt (déjà ?) par des Intelligences Artificielles, nous n’aurons plus d’inconnus ou de secrets pour personne

“

Les machines en sauront plus et mieux que nous-mêmes sur nous-mêmes.

3) AVANTAGES & INCONVÉNIENTS DES ASSISTANTS VIRTUELS

Néanmoins, listons donc quelques avantages de ces assistants

- Possibilité de répondre à des questions de type :
  - Connaissances générales
  - Actualité
  - Météo
- Jouer de la musique ou des sons d'ambiance
- Aider à la réalisation d'une recette de cuisine
- Procurer une nouvelle forme de jeu
- Faire des échanges vidéo
- Afficher des pages Web suivant des mots-clés vocaux de recherche

Et listons, sans pouvoir être exhaustif, les problèmes et inconvénients générés par ces assistants

- Écoute permanente par le micro
- Aucune garantie pour savoir quoi, combien, à qui, à quelle fréquence des bouts ou des intégralités de conversation peuvent être envoyés
- Détection des émotions portées par le son de la voix
- Détection de l'état émotionnel suivant l'analyse des contenus prononcés
  - Richesse et vocabulaire employé
  - Rapidité – lenteur des mots prononcés
  - Placement des accents toniques ou espacements dans les syllabes
  - Comparaisons avec l'historique connu

- Détection de la confiance accordée à une personne ou à une marque par l'analyse de la manière dont sont prononcés le nom et les mots associés
- Possibilité de savoir à travers la reconnaissance faciale ou d'autres objets (montre, téléphones, etc.) qui est dans la pièce.
- Analyse des déplacements
    - Qui ?
    - À quelle heure ?
    - À quelle vitesse ?
    - Quelle forme de parcours ?
    - Quels écarts par rapport à d'autres déplacements
- Possibilité de détection d'autres événements situés en-dehors du champ de vision comme une porte qui claque ou qui s'ouvre.
- Analyse des liens entre températures dans la pièce et état émotionnel
- Détection des objets utilisés ou consommés. La reconnaissance faciale ne sera pas que pour les personnes, elle saura aussi utiliser pour savoir ce que l'on mange, à quelle heure et comment !
- Ajoutons également tous les sujets abordés ci-dessus, mais avec la possibilité que des
    - Personnels non autorisés de parties tierces comme des sous-traitants des fabricants des appareils accèdent aux données
    - Ou des hackeurs de type gris, noir ou arc-ciel inversé se mettent aussi à détourner les données pour leur plus grand profit.
- Des comportements bizarres commencent à voir le jour… (En Anglais).
- Et sans doute plein d'autres possibilités de surveillance ou d'analyses …

Alors faudrait-il pouvoir se passer des avantages de la modernité pour ne plus avoir les inconvénients ? Faut-il renoncer au progrès ou se rendre pieds et poings liés aux grandes puissances numériques ?

Il y a 2 solutions pour se sortir de ce dilemme.
Comme à l'habitude, on a du factuel et du stratégique.

a) LE FACTUEL

En premier, on peut décider, voire **surtout imposer**, que l'écoute de ces appareils ne soit pas permanente et qu'elle soit contrôlée et décidée par les utilisateurs.

Il n'y a AUCUNE raison pour que ces appareils ne soient pas vraiment contrôlables par leurs utilisateurs. C'est uniquement la volonté des constructeurs de les livrer

avec ce type de fonctionnement. Et la passivité des services publics de chaque nation de laisser de tels produits pénétrer dans nos maisons.

Mais comme on l'a vu, c'est une réponse factuelle.
Et c'est aussi une réponse limitée.

Car même si l'utilisateur contrôle et limite les temps et possibilités d'écoute, rien n'empêchera les transmissions de données, qu'elles soient ou non prévues par le constructeur. Et rien n'empêchera les analyses de ces données et les ventes de ces analyses à qui que ce soit.
On a donc limité par cette approche que factuelle, comme bien souvent, le ou les problèmes, mais on ne les a pas résolu.

Pour cela il faut passer à une autre étape.

b) LA RÉPONSE STRATÉGIQUE : LE PROXY NATIONAL

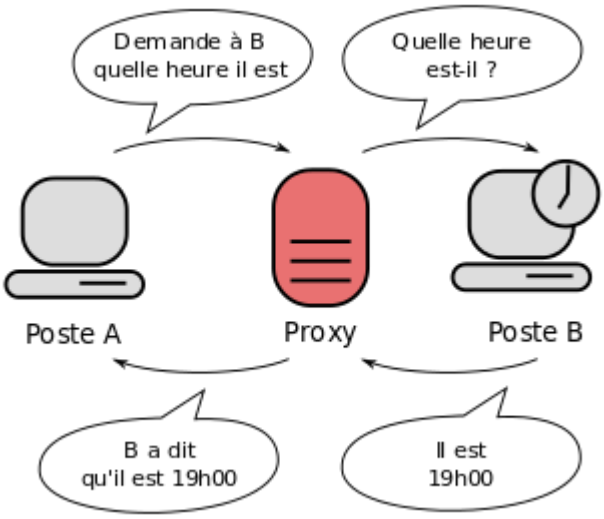
Si l'on veut un véritable contrôle sur les données numériques collectées, il faut rester cohérent et également utiliser des outils informatiques et notamment des outils de réseaux informatiques, car c'est là que se situe le va-et-vient entre les assistants et les serveurs des constructeurs.

Et c'est là qu'intervient la notion de Proxy réseau.
Sans rentrer dans trop de détails ni de technique, ce qui serait doublement inutile, nous pouvons simplifier le concept du Proxy par la notion d'intermédiaire. Dans le cadre d'un Proxy réseau, c'est un passage obligé pour qu'une demande formulée par un appareil (poste A) arrive bien à l'appareil visé (le Poste B). Ce passage est obligatoire. Techniquement parlant A ne peut parler à B que via l'intermédiaire et B ne peut répondre à A toujours que via l'intermédiaire.
On trouve ce type de schéma dans beaucoup de schémas informatiques de type client-serveur notamment pour la consultation de pages Web, mais aussi pour l'envoi de données informatiques au sens large. Et ce pour différentes raisons dont la sécurité entre machines et la possible accélération des échanges par le biais de cache de type Web.

En simplifiant, la mise en place d'un tel équipement permet d'avoir un intermédiaire qui va vérifier et valider que ce que vous transmettez comme informations depuis les assistants présents dans votre maison ne sont pas confidentielles, en-dehors des

lois et conformes à ce que vous souhaitez transmettre.

Mais ce qui nous intéresse aussi dans le cadre d'un déploiement d'un Proxy national pour les assistants vocaux, c'est une autre des propriétés des proxys, la confidentialité.



Sur https://fr.wikipedia.org/wiki/Proxy

4) CONFIDENTIALITÉ PAR LE PROXY NATIONAL

En effet les Proxys offrent la possibilité, au moins théorique, de « masquer » l'identité de celui qui fait la demande. Par identité il faut comprendre non pas forcément le nom et adresse de l'utilisateur, mais son équivalent en réseau informatique, à savoir son adresse IP et son empreinte numérique (voir l'article d'Avira sur le sujet qui prêche pour sa paroisse).

Ainsi dans le cadre des avantages (nécessités ?) à mettre en place, pour chaque pays, son propre Proxy national pour les assistants vocaux, la confidentialité vient en premier.

Le Proxy national permettra de masquer l'identité numérique, au sens large (Adresse IP et empreinte numérique), de l'utilisateur auprès du fabricant de l'assistant afin de diminuer et contrôler le profil marketing utilisé par ce dernier. Car à part les achats en ligne pour identifier son client, qui a vraiment besoin de savoir dans le détail qui vous êtres et ce que vous avez vu, fait ou demandé

précédemment sur Internet ?

Également les données envoyées aux serveurs des constructeurs via le proxy seront contrôlées pour ne laisser passer que des phrases – ordres – demandes en bonne et due forme avec l'inclusion obligatoire du mot-clé du fabricant (Alexa, Google, Mark, Skynet…). Tout ce qui ne sera pas légitime sera filtré et ne sera pas envoyé aux serveurs des constructeurs.

Dans le même principe, les informations de type Métadonnées qui sont recueillies hors micro et caméra seront vérifiées et approuvées avant d'être envoyées aux serveurs des constructeurs. Ainsi on peut admettre que l'envoi d'informations clefs comme une géolocalisation large et une heure locale précise sont possibles. (Cela permettra au moins à tous ceux qui vivent dans des abris antiatomiques de pouvoir poser légitimement la question clef « Quel temps va-t-il faire ?)

Pour l'instant ces Métadonnées semblent être limitées, mais au fur et à mesure du développement de ces assistants virtuels, elles vont s'enrichir et il faudra les encadrer de mieux en mieux.

Un autre avantage possible de l'utilisation d'un proxy est la possibilité de faire des vidages de cache informatique très régulièrement (à chaque demande ?) pour protéger au mieux la confidentialité des demandes.

Les temps de traitement informatique de transfert par des Proxys seront de plus en plus négligeables dans le cadre des déploiements continus de la fibre optique et de la 5G puis de la 6G et autre XG qui vont venir petit à petit se répandre sur l'ensemble du globe. Encore une fois ne pensons pas simplement en termes d'années, mais de dizaines, centaines, voire en milliers.

a) DE NOUVEAUX SERVICES COLLECTIFS

On pourrait également profiter de la mise en place d'un tel Proxy pour créer une Banque Nationale de données récoltées et entièrement anonymisées, aux objectifs et méthodes clairs, collectant et structurant certains types d'informations qui pourraient être utiles à la Collectivité. À condition que cela soit strictement encadré et possible techniquement (voir plus bas).

On pourrait ainsi mettre en place via ce Proxy national de nouveaux services où les demandes seraient interceptées et traitées uniquement par le Proxy. (« Alexa

appelle les Pompiers ! » ou « je fais une crise cardiaque »). Le fait de savoir, comme dans un appel classique par téléphone, d'où vient la demande responsabilisera les personnes. Et on pourra même imaginer un mini dialogue via l'assistant vocal comme lors des appels au SAMU pour bien valider l'envoi d'une équipe sur place.

Toujours dans ce même cadre de services supplémentaires chapeautés directement par le Proxy, on pourrait faciliter la demande de documents administratifs (je certifie demander un extrait de naissance. Mon code de validation est le …).
Plein d'autres potentiels sont possibles.

En quelque sorte, sur la base de produits venant d'entreprises privées, en ajoutant un service national, le Proxy, on peut développer de nouveaux avantages et possibilités à l'ensemble des membres de la Communauté. Il y a bien une alliance possible entre les initiatives privées et les Biens COOPÉRACTIFS.

b) LES OBJECTIONS AU DÉPLOIEMENT

Tout d'abord, pour rappel, pour ne pas alourdir le propos et pour être compréhensible par le plus grand nombre, bon nombre d'aspects techniques purs ne sont pas décrits dans cet article. Ce n'est pas le but. L'essentiel est d'avoir l'information que ce type de service, le Proxy national de filtrage et de protection de confidentialité est tout à fait réalisable. Surtout si en plus on impose aux fabricants des contraintes logicielles et spécifiques aux constructeurs pour que leurs appareils soient aux normes en vigueur.

Une autre objection pourrait être le coût du déploiement d'un tel dispositif.
Mais ne dit-on pas que la liberté n'a pas de prix !
Il aussi voir ce dispositif comme un moyen de protection et de sécurité. Les voitures coûtent un peu plus cher avec des ceintures de sécurité, mais tout le monde a bien compris maintenant l'importance de leurs présences. Il en sera de même pour le Proxy national.

Mais la principale objection, et légitime, pourrait de faire remarquer que le déploiement d'un tel dispositif reviendrait à mettre en place une surveillance d'État. Passons outre le fait de s'étonner que ceux qui s'inquiètent d'une surveillance d'État ne sont pas révulsés et révoltés par la même surveillance exercée par des entreprises privées, et qui plus est étrangères (actuellement qu'Américaines) pour proposer des réponses nécessaires à cet argument.

Une fois que l'on a dit que l'accès aux données à leurs exploitations serait strictement encadré par des textes de lois, des normes, des règles et également la présence d'une institution indépendante, on aura confirmé l'esprit que l'on souhaite implanter dans le dispositif. Mais on n'aura pas avancé sur les preuves et efficacités des barrières de protection que l'on souhaite mettre en place.

C'est à ce moment-là qu'il faut retourner dans des aspects purement techniques. Toujours pour rester le plus compréhensible possible, nous ne rentrerons pas dans les détails de mise en place, mais nous mentionnerons au moins deux mécanismes de barrière de protection.

Premièrement, à la différence de ce qui peut se passer chez certains constructeurs (qui le sait vraiment ?) il n'y aura pas de mise en mémoire de tous les éléments demandés par les utilisateurs. Il n'y aura pas de Silo de Data. Rien de ce qu'aura demandé un utilisateur ne sera conservé. [De plus cela fera des économies de frais de stockage à modérer avec le nombre de métadonnées que l'on peut décider de garder dans le temps pour des usages bénéfiques à la Communauté].

Deuxièmement, on peut (doit ?) organiser l'envoi des informations sonores transmises par les assistants en place chez les utilisateurs sous forme de données cryptées qui sont envoyées au Proxy qui renvoie ces mêmes informations cryptées aux serveurs des constructeurs. Et qui en retour vont retourner au proxy de nouvelles informations cryptées que seul l'appareil émetteur de la demande pourra décoder et donner une réponse en clair à l'usager. Et ce quelle que soit la forme de la réponse (Sons, vidéo, texte). À aucun moment le Proxy national ne verra l'intégralité des demandes faites par les utilisateurs, mais on aura bien quand même accès à des parts de la demande, ne serait-ce que pour vérifier que l'appel à l'assistant a bien été déclenché par l'utilisateur (Alexa ?) et que les métadonnées recueillies et transmises par les assistants respectent bien les normes de confidentialité édictées.

La mise en place de tel mécanisme nécessite des déploiements et approbations de Clef de cryptage telles que des clefs privées ou publiques, mais, encore une fois, le sujet de l'article n'est pas la description technique de la mise en place du proxy, mais de la possibilité et nécessité de sa mise en place

c) LE TIMING POSSIBLE

Attention, les assistants actuels ne sont pas forcément prévus ou compatibles avec

un tel mode de fonctionnement comme énoncé plus haut. Il faudra imposer, pour chaque pays, une date où aucun assistant ne pourra être vendu s'il n'est pas aux nouvelles normes décrétées. Et une autre date (car le sujet est différent) où aucun ancien type d'assistant vocal ne pourra être utilisé ou opérationnel chez les clients [de toute manière à la vitesse où les fabricants ~~imposent~~ gèrent leur obsolescence programmée, cela ne pourra être qu'une question de mois].

d) LES ENJEUX

Ils sont colossaux et décisifs.

“

Si le Citoyen n’a pas le contrôle de ce qui se passe

dans sa propre maison, si un État ne contrôle pas ou ne sait pas ce que les Entreprises privées collectent comme informations chez ses propres Citoyens alors les notions d'indépendance et d'autonomie pour ce pays et ses habitants sont à risque.

Et sans indépendance et autonomie, il **n'y a pas de vraie Liberté** possible.

En matière de Numérique, il y a **3 grands terrains**, des champs de bataille entre les sociétés privées pour s'emparer de l'ensemble des activités humaines.
– Le bureau. C'était l'époque des premiers ordinateurs et la domination de Microsoft.
– L'extérieur. C'est tout ce que l'on fait entre le bureau et sa résidence. C'est l'époque qui commence véritablement avec les années 2 000 et la démocratisation du téléphone portable. C'est l'ère de Google via Android. À noter qu'une frange de ce champ de l'extérieur se déroule maintenant à travers la voiture connectée et autonome.
– L'intérieur. C'est tout ce que l'on fait dans sa maison.

Bien évidemment, tout s'interfère un peu. On peut faire du téléphone portable (Google) chez soi et travailler avec un ordinateur (Microsoft) mais voir les luttes pour la domination numérique à travers des typologies géographiques permet de mieux comprendre les mouvements stratégiques en cours.

Ainsi les Assistants vocaux sont donc dans le terrain de l'intérieur, celui de la Maison. Avec toutes les répercussions par le développement de la domotique. Tous les objets seront connectés. Connectés entre eux et connectés à vous. En permanence. Avec des dialogues, des échanges, des ordres de plus en plus pertinents et précis. On trouve un exemple de ce développement dans la page de ce qu'appelle Amazon les « skills » (aucun effort de traduction et d'adaptation du mot en langue Française. Ou dans les autres langues. Apparemment dans une indifférence quasi générale tellement cet état de fait, absence de traduction, semble être toléré. C'est comme si, en Français, on employait maintenant le mot computer à la place d'ordinateur. Bref ..) Ils sont en constante progression et c'est une lutte commerciale entre Amazon, Facebook, Google, Apple, Microsoft et bientôt les Géants Chinois du Numérique.



Amazon Echo @rohane

> *Après l'écrit et le visuel, ne laissons pas les Sociétés Privées mettre la main sur le dernier champ de bataille Numérique en cours, celui du vocal.*
>
> *— ALPHAPOLIS*

Nous visons sur ce plan une période passionnante pour les amoureux des grandes manœuvres technologiques et commerciales. Mais nous vivons encore dans l'ancien. Il y a beaucoup d'efforts faits, d'énergies perdues, de temps gaspillé, pas d'intelligence collective et pas de vision stratégique.
Heureusement une autre réalité peut être créée. Et vécue.

4) LES RÉPONSES

Elles sont de trois niveaux possibles. Nous en présentons trois dans cet article (*le 4ième niveau sera évoqué dans un autre article au sujet plus global*).

– La Loi. On a vu que cette réponse était plutôt de type défensif. Et qu'en plus de devoir exercer un contrôle permanent (par quel moyen technologique ?), cela ne résout pas les questions de fond qui sont la collecte et l'exploitation des données.

– Le Proxy. Cette réponse qui est principalement développée dans le cœur de l'article va plus loin et commence à renverser la vapeur en contrôlant ce qui est transmis aux constructeurs ou exploitants des Assistants. C'est une réponse qui est active et qui encadre, techniquement (et c'est bien plus sûr que des simples décrets ou articles de Lois) les comportements de ces mêmes constructeurs.
C'est une bonne démarche, constructive.

Mais de manière temporaire. C'est plus une étape intermédiaire avant la meilleure réponse sur le fond. En effet, dans ce schéma, il y a toujours la possibilité d'un temps de retard par rapport aux développements poussés par les constructeurs. Plus la petite musique habituelle de « vous nous bridez l'innovation, on ne peut plus développer de nouveaux services, c'est la fin du progrès, patin couffin » qui ne tardera pas à venir.

5) LA FORME DE LA RÉPONSE

Il faut donc une réponse stratégique sur le fond, la forme et la durée.
C'est le troisième niveau.

Cette réponse ne passe que par les Biens COOPÉRACTIFS et par un de ses outils, l'Open Source ou le Logiciel Libre (la différence selon Richard STALLMAN) Et ce même s'il est probable que l'organisation économique de l'Open Source doit évoluer pour répondre aux nouveaux défis auxquels elle fait face, l'utilisation de ses

créations sans contrepartie financière (c'est un autre sujet).

En effet, seule une organisation la plus Universelle possible, sous la forme de Biens COOPÉRACTIFS, allant plus loin que les proxys nationaux, peut permettre un développement optimum pour tous de cette évolution que sont les Assistants vocaux ou de Maison.

Mais il faut un système, une organisation où :
– Les services ne sont pas bridés dans les inventions et innovations.
– Tout en respectant la confidentialité et vie privée des utilisateurs
– Tout en permettant au plus grand nombre possible de développeurs (et pas forcément de grandes sociétés privées et encore moins d'Oligopoles) à pouvoir apporter leur contribution dans l'amélioration de ces services
– Tout en permettant au plus grand nombre possible de constructeurs indépendants de proposer leurs modèles ou accessoires
– Tout en permettant aux utilisateurs (pour ceux que cela intéresse et motive) de modifier ou améliorer les matériels et les logiciels
– Tout en permettant à la collectivité, dans le respect de la confidentialité et de l'anonymat, de recueillir des informations importantes et parfois structurantes pour d'autres biens communs.
– Tout en permettant la création ou le développement de nouveaux services à travers ces assistants comme (voir plus haut) la demande de papier administratif. Mais on peut imaginer des prises de rendez-vous ou des dialogues avec des « Robots » ou « Intelligence Artificielle » pour faire avancer ou résoudre tel ou tel point. Sans parler des interactions avec les objets connectés de la maison ou d'autres lieux.
Tout est à imaginer et à mettre en place pour le plus grand bien de tous.

Ce déploiement sous la forme de multiples Biens COOPÉRACTIFS qui travailleront entre eux en toute coopération et intelligence passera par des édictions de Normes techniques et d'articles de Lois (dont les bases communes devront être partagées le plus possible entre les pays), pour demander, imposer et contrôler le fonctionnement et l'ouverture de ces assistants.

6) LA BASE DE LA RÉPONSE

La première des urgences consiste donc, comme cela a été fait pour le Web (ce qui explique d'ailleurs son succès) à créer des Protocoles communs de discussion et de

dialogue entre les équipements.



Code en langage dit assembleur

> *Il faut créer une* **Langue Technique Commune** *entre tous les appareils et logiciels relatifs aux Assistants vocaux et Objets connectés.*
>
> *— ALPHAPOLIS*

Une Langue que tous ces appareils devront parler et comprendre.

Une Langue qui pourra évoluer, s’améliorer, s’enrichir.

Une Langue que tout constructeur devra utiliser. Ce sera une Norme obligatoire.

Une Langue dont le développement, la sécurisation, seront financés par une participation commune et minime prélevée sur toute vente de matériel ou de logiciel utilisant la Langue. (rappelons que l’usage de la langue est obligatoire pour tous les appareils et logiciels/applications)

Il n’y aura pas une Langue Amazon, une Langue Google, une Langue Xiaomi, etc .. Il y a une seule langue technique pour que tout le monde communique avec tout le monde et que tout le monde puisse comprendre tout le monde.

Quand on voit les bénéfices, dans tous les sens du terme, que les protocoles du

Web (Ici pour l'Hypertext Transfer Protocol) ont apportés à l'ensemble de l'Humanité (et aussi des bénéfices financiers aux actionnaires des GAFAM et BATX), on voit à quel point un langage Commun, des protocoles techniques, permettront de faire progresser la qualité et la richesse de vie et de possibilités de créations au plus grand nombre.

De plus, avec l'expérience, réussie, du World Wide Web et des organismes qu'il a générés comme le World Wide Web Consortium et l'Internet architecture Board, nous savons mieux comment structurer et protéger ces types de Biens COMMUNS.

Alors à nous de créer cette Langue technique commune des assistants vocaux !

Post Scriptum et mises à jour

Ne trompez pas votre compagne ou compagnon , Alexa enregistre tout !
Une aventure transformée en mésaventure rapportée le 10 octobre 2022 par le site Presse-Citron.

L'assistant vocal en tant qu'appareil dans la maison va t-il devenir le futur répondeur téléphonique ? Après un engouement initial, le soufflé d'intérêt et d'usage semble retomber

Même Amazon, le 11 novembre 2022, s'inquiète de la rentabilité de son outil.

Et META, au 16 novembre 2022 semble bien parti pour arrêter, totalement, son activité dans le domaine des assistants personnels sous forme d'objets.

Le 2 janvier 2023, pour bien commencer l'année , c'est la découverte d'une faille chez un concurrent d'Alexa, les enceintes Home de Google.

On soupçonne Alexa, en mars 2023, d'avoir recueilli des données personnelles d'enfants, risquant ainsi une très lourde amende, aux USA.

Et en Mai, fais ce qu'il te plaît. C'est ce que s'est dit Alexa qui a décidé d'intégrer de l'Intelligence Artificielle pour se donner du Tonus.

Mais il n'y a pas qu'Alexa d'Amazon qui ait des malheurs; Google en a également. Annonce en juin 2023 de l'arrêt de service de Google assistant pour des millions d'appareils.

Surfant sur la vague de l'IA, Amazon proclame en juillet 2023 que son assistant personnel, Alexa, sera plus intelligente. Ce qui veut dire que l'ancienne version l'était moins…

Et en septembre 2023, puisqu'il semble qu'au nom de la nouvelle idole informatique, l'IA, on peut tout se permettre, Alexa se met, par défaut (consentement implicite), à écouter et retenir, nos conversations, pour créer et développer son Modèle de Langage interne.

Mauvais vent possible pour Alexa en Novembre 2023 avec une prévision de nombreux licenciements dans l'équipe.

On espère en janvier 2024 chez Alexa que l'IA générative va lui sauver la mise. Mais pour l'instant ça patine dur…



Philippe AGRIPNIDIS

Cocréateur de Biens Communs

La Coopération pacifique et fructueuse est une preuve d'évolution et de maturité de Civilisation

