

# Dans 5 ans, plus aucun mot de passe ne résistera aux calculs de haute performance.

[Émilie Bonnefoy](#) est Co-fondatrice & CEO d'[OPEN SEZAM](#) ?, membre du [Cercle des Femmes de la Cybersécurité](#) et auditrice [IHEDN](#) Majeure SNC 2022-2023

*1/ Un récent article révèle que [les hackers embauchent plus de femmes que les entreprises de cybersécurité](#). Qu'est-ce que cela vous inspire ? Serait-ce le point culminant de la parité ? Les femmes seraient-elles donc aussi capables que les hommes de nuire ?*

Je découvre ces chiffres à la lecture de l'article et comme probablement beaucoup de lecteurs j'imagine, ils m'interpellent. La problématique de la parité et plus globalement de la mixité des équipes dans les entreprises de sécurité est systémique. Elle démarre dès le cursus scolaire à travers les choix d'orientation et se poursuit dans la composition des équipes ensuite. On observe toutefois à travers ces chiffres que les femmes ont un attrait certain pour la cybersécurité à condition que leurs compétences et le cadre de travail offert leur permette de s'épanouir. Et je regrette ici que certaines d'entre elles choisissent de basculer du côté "obscur" de la force. On imagine aisément ce qui peut être attrayant : travailler de chez soi, dans un environnement plus feutré, plus caché, plus libre car offrant souvent l'anonymat ou la pseudonymisation, sans véritable hiérarchie et probablement avec une rémunération équivalente à celle des hommes délivrant le même service.

Cela doit nous faire réfléchir sur deux choses :

Le cadre de travail et la culture dans l'entreprise sont-ils adaptés ? Le management est-il enclin à mettre en place un cadre de travail "sain", c'est-à-dire et sans tomber dans le puritanisme, un cadre permettant à chaque salarié de se sentir valorisé pour ses compétences et ses qualités humaines ?

La structuration des équipes dirigeantes permet-elle d'intégrer cette problématique ? Regardons les comités de direction des 20 plus grandes entreprises de cybersécurité, combien de femmes au board ? C'est une bonne chose de faire de la sensibilisation, de financer des programmes associatifs, mais le plus efficace reste de montrer l'exemple. On connaît désormais l'efficacité des rôles modèles. Si on s'abstrait de l'aspect moral du raisonnement, c'est également une hérésie en terme de business. Comment favoriser l'adoption de bonnes pratiques ou de produits cybers lorsque ceux-ci sont uniquement développés par une catégorie de la population ? Cela pose aussi des questions sur l'efficacité des solutions mises en œuvre pour favoriser la résilience des organisations face au risque cyber.

*2/ Alors comme ça, vous allez enfin nous libérer du mot de passe ?*

C'est effectivement l'ambition d'Open Sezam entreprise à mission de cybersécurité. 3 raisons à cela. Ils sont d'abord le premier vecteur des

cyberattaques et à ce titre, un vrai frein dans la confiance que l'on peut avoir dans les usages numériques. La seconde raison tient aux grandes ruptures technologiques auxquelles nous nous préparons : dans 5 ans, plus aucun mot de passe ne résistera aux calculs de haute performance. Derrière chaque innovation de rupture (l'IA, le quantique...) il y a un usage détourné par les cyber-attaquants.

Enfin, l'Union Européenne et le gouvernement français sous l'impulsion de la Présidence européenne ont préparé une feuille de route ambitieuse pour accompagner nos organisations d'importances vitales, nos services essentiels, nos entreprises et en particulier nos PME vers une plus grande résilience face à un risque cyber croissant.

Pour les éditeurs de logiciels dont nous faisons partie, cela implique la nécessité de faire preuve d'une forte capacité d'innovation pour proposer des solutions simples d'usage, simples à déployer et adaptées à des cas d'usage de plus en plus complexes. C'est ce que nous faisons chez Open Sezam. Nous permettons aux entreprises de libérer les utilisateurs de leurs mots de passe grâce à une plateforme ultra-simple à déployer : nous nous interfaçons dans le système existant, de façon transparente. Les utilisateurs peuvent ensuite s'authentifier via un magic link ou via n'importe quel device grâce au lecteur de biométrie. L'UX de notre plateforme est simple et agréable tout en contenant les informations clés liées à la fréquentation des applications sur lesquelles nous déployons notre solution.

***3/ Nos solutions françaises sont-elles condamnées au succès d'estime ou peuvent-elles, elles aussi, prétendre à une adoption massive dans le monde ?***

C'est vrai que si l'on regarde le paysage des solutions cyber massivement adoptées sur le marché de la cybersécurité par exemple dans les différents cadrans Gartners, les acteurs français sont très minoritaires.

Plusieurs explications sont souvent avancées : le manque de soutien à l'innovation ou à l'internationalisation. On pense souvent au marché américain, très dynamique et très alimenté par les Israéliens qui y déploient nombreuses de leurs solutions.

Mais le marché européen est extrêmement important en volume. Ceux de l'Afrique et de l'Asie sont aussi identifiés par les experts comme de futurs marchés de masse.

Certains géants de la tech comme AWS sont devenus des acteurs incontournables dans notre secteur. Ils ont bénéficié d'un fort soutien du gouvernement américain qui ne cache pas ses actions préférentielles dirigées vers les entreprises nationales. 1er fournisseur de Cloud au monde, AWS a créé le marché en invitant le concept de Cloud Public. Misant sur ses fortes capacités techniques et ses capacités à tirer le fruit de son expérience avec sa plateforme d'e-commerce, l'entreprise est devenue une machine de guerre. L'attention portée au client, la mise en oeuvre de services ultra-simples d'usage qui permettent de réserver des instances avec une simple carte de crédit, c'est un peu comme un Mac-Do le dimanche soir : facile, pas si bon

marché que ça mais c'est aussi le juste prix de la tranquillité.

En France et plus globalement, nous avons des personnes brillantes sur le plan technique, des entrepreneurs visionnaires, des sources de financement. Il faut simplement que nous prenions conscience que Rome ne n'est pas faite en un jour et arrêter de renoncer en pensant que la bataille est perdue.

**4/ Vous avez une formation de juriste en droit public (des gens très bien !). Comment cela a-t-il orienté votre activité vers un sujet de souveraineté ?**

J'ai choisi sans vraiment choisir. Le jour où j'ai mis un pied dans l'amphithéâtre j'ai regretté de ne pas avoir choisi une formation scientifique. C'est terrible, tout m'intéresse et je trouve que malheureusement nos formations ne soient pas plus transversales, plus éclectiques, notre monde est devenu tellement complexe...

J'ai cependant adoré ces années et en particulier la rigueur du syllogisme juridique, l'enjeu de protection de la chose publique qui mène vers la notion d'un intérêt à celui des individus : l'intérêt général. Le sujet de la souveraineté, c'est celui d'un Etat qui ne dépend pas d'un autre ou tout du moins qui consent à ses dépendances. C'est l'objectif d'atteindre le plus haut niveau d'indépendance possible pour décider et agir dans le respect de nos valeurs et de ce que l'on qualifie souvent de besoins vitaux. C'est un sujet qui m'a toujours passionné et qu'aujourd'hui je peux approfondir dans le cadre d'un cycle d'auditrice à l'IHEDN, une institution extraordinaire qui regroupe des dirigeants, des militaires, des cadres de l'Etat avec cette logique de décloisonner les réflexions et de proposer des actions concrètes au Secrétariat Général à la Défense et à la Sécurité Nationale dans un contexte de plus en plus complexe.

**5/ Comment décririez-vous le rapport que nous entretenons en France avec les technologies venant de l'étranger, des Etats-Unis ou de la Chine ?**

Un rapport un peu similaire avec celui du fast-food du dimanche soir : on sait que ça peut nous coûter un jour (notre autonomie de réflexion et d'action par exemple), que ça n'est pas si bon marché, que ça alimente un système assez précarisant...mais on s'en satisfait : c'est pratique, facile avec un goût doux et ça répond au besoin de se nourrir.

Malheureusement, ce ne sont pas simplement des technologies que nous importons. Ce sont aussi des usages et une certaine vision du monde – comme par exemple celui de la propriété des données.

**6/ Prévoyez-vous l'atrophie de la mémoire humaine ?**

Je suis presque trop optimiste pour imaginer ça ! Et puis il faudrait solliciter les grands spécialistes du sujet : les neurologues mais aussi les spécialistes en sciences cognitives. Sur ce plan, je vous recommande le livre de Gérald Bronner "L'Apocalypse Cognitive" qui montre comment le déferlement d'informations et la "dérégulation du marché cognitif" nous exposent à un risque civilisationnel en s'attaquant à notre cerveau.

**7/ Pourquoi avez-vous choisi de développer une solution d'authentification plutôt qu'un déodorant sans paraben ou une marque de chaussettes bio ?**

Ce sont surtout les rencontres et ce que j'ai découvert en étudiant la question de la gestion des accès et des identités. Les Anglais diraient : "What a mess" ! L'authentification, c'est le point de départ de tout, c'est la porte d'entrée de la maison. A quoi bon mettre en place une alarme, des barbelés, des barreaux aux fenêtres si la porte d'entrée de la maison reste ouverte ?

J'utilise du déodorant sans paraben et il m'arrive de porter des chaussettes bio. Si l'enjeu était aussi important que celui de la sécurité de nos usages numériques pour que la digitalisation soit vraiment un progrès pour notre humanité, je me serais posé la question ?

J'ai aussi la chance de travailler entourée d'amis brillants, curieux, qui ont soif d'apprendre et d'une grande humilité. Nous avons de grandes ambitions communes pour un projet qui a un fort impact sociétal.

**8/ La biométrie peut impressionner. D'un côté, elle permet de s'affranchir des artefacts ou ces fichus mots de passe. Mais d'un autre, nous devons nous-même devenir ce moyen de tout sécuriser. Comment voyez-vous la ligne médiane entre ces deux chemins ?**

Il est vrai qu'il faut être extrêmement vigilant sur l'usage de la biométrie et en France, nous avons la chance d'avoir des organismes étatiques comme la CNIL ou certains organismes de recherche comme l'INRIA qui étudient et mesurent le risque de compromission lié au stockage distant de données biométrique par exemple. Certains films d'anticipation sont assez proches de ce que l'on peut faire. Et il est donc absolument nécessaire que certaines autorités morales contrôlent le cadre déontologique de la mise en œuvre de ces technologies. Et donc parfois la question se pose de savoir si la sécurisation est bien légitime au regard du risque encouru.

S'il s'agit d'une problématique d'adoption de l'usage, le mot de passe peut aussi être remplacé par d'autres techniques comme par exemple ce que l'on appelle le "lien magique".

Cela soulève une question fondamentale : quel niveau de sécurité un individu est-il prêt à accepter compte tenu du niveau de risque et comment en tant qu'éditeur de logiciel nous trouvons le juste équilibre.

**9/ On parle beaucoup de décentralisation en ce moment. Pensez-vous que cela peut avoir des conséquences politiques, comme un essor du concept de « souveraineté personnelle » par exemple ?**

La décentralisation – et en particulier la décentralisation de l'identité que nous étudions de près chez Open Sezam – est une excellente opportunité de redonner du pouvoir aux individus sur l'usage de leurs données. C'est un domaine dans lequel nous avons en tant qu'européens une vision singulière et qui s'est illustrée par l'introduction du RGPD ou plus récemment par l'adoption du DMA et du DSA. La décentralisation permet également une meilleure gestion du risque pour les organisations soumises à des obligations légales et réglementaires.

L'Union européenne a demandé aux États européens de mettre à disposition un portefeuille numérique mais on voit que c'est très compliqué – techniquement et politiquement – d'aboutir à des solutions satisfaisantes tant pour les pouvoirs publics que pour les utilisateurs in fine. Dans un contexte d'hyper-digitalisation et aujourd'hui dominé par le modèle des plateformes spéculant sur l'exploitation des données, je pense que cette transition sera inévitable. La réglementation ne suffira pas et devra être nécessairement soutenue par des solutions technologiques.

*10/ L'application que vous conservez dans votre téléphone sur une île déserte (Pas de 4 ni de 5G ni évidemment de prise électrique). Trêve de plaisanterie : quel ouvrage ?*

Le Meilleur des Mondes d'Aldous Huxley !