CONFIANCE NUMERIQUE ET GOUVERNANCE DIGITALE

Par David Commarmond

Veille
www.veillemag.com
Le magazine des professionnels de l'information stratégique

Livre Blanc

Confiance Numerique et gouvernance digitale. Juin 2O24

Auteurs
David Commarmond
Jacqueline Sala
Anna Elviro

Soyez partenaire de notre prochaine mise à jour. Merci de contacter dcommarmond@veillemag.com

Sommaire

01. EDITO. “INTELLIGENCE ECONOMIQUE, DURABILITÉ, CYBERSÉCURITÉ, DES ÉTUDES DE CAS SIMILAIRES”.

Aujourd’hui, tout comme la durabilité en son temps était considérée comme un enjeu secondaire, la confiance numérique est venue sur le devant de la scène. Les dirigeants qui ont connu l’expérience amère d’une cyberattaque et qui ont vu leur entreprise perdre des actifs en raison de l’absence de procédures de sécurité adéquates en mesure toutes les conséquences et y prêtent ensuite une attention particulière.

Dans ce contexte, il convient d’analyser et d’évaluer les risques, et d’informer les collaborateurs et les clients des opportunités et des nouveaux dangers liés à l’intelligence artificielle et aux enjeux numériques de sécurité et de stockage de données.

En effet, sur le terrain, la confiance numérique est cruciale pour les entreprises évoluant dans un paysage numérique complexe. C’est aussi au niveau macroéconomique une question de souveraineté numérique et de protection des actifs stratégiques nationaux.

De nouvelles législations pour se protéger, nécessaires, mais insuffisantes :

Un savant mélange et subtil équilibre entre les contraintes législatives, complexité et libertés pour les différents acteurs et intérêts souvent contradictoires. Parmi les priorités, nous insistons sur la nécessité de naviguer dans le paysage législatif cohérent, en veillant à ce que les entreprises y compris étrangères respectent toutes les réglementations pertinentes.

Des atteintes à la souveraineté dans de nouveaux risques, de nouveaux acteurs :

Enfin, il est important de noter que l'utilisation de plateforme d'intelligence artificielle peut entraîner la divulgation de données sensibles, un danger majeur. Les entreprises doivent prendre des mesures pour protéger leurs données.
Aujourd'hui les chefs d'entreprises ne sont plus seuls. De nombreux acteurs étatiques comme l'ANSSI, la Police, la Gendarmerie, la Justice, les Ministères notamment Bercy ont développé toute une gamme d'outils et de services pour répondre aux attaques venant de l'étranger. C'est fondamentalement différent. La multiplicité des attaques réussies ou stoppées sont autant de leçons qui mettent à l'épreuve notre tissu économique et sa résilience. Le défi demeure cependant de convaincre plus de chefs d'entreprise et plus rapidement : **le facteur temps joue contre nous.**

David Commarmond

02. QU'EST-CE QUE LA CONFIANCE NUMÉRIQUE ET QU'EST-CE QU'ELLE N'EST PAS ? .

Avec le développement des échanges par voie dématérialisée et la transformation numérique est apparu rapidement le besoin d'assurer la sécurité des échanges dans ce qui est devenu le cyberespace. C'est alors que **la notion de confiance numérique** est apparue et englobe plus largement : la sécurité des canaux, la fiabilité des informations échangées ainsi que le respect de la vie privée des citoyens.

C'est ainsi que l"Anssi définit en Octobre 2023 la confiance numérique comme "***les éléments consécutifs de la transformation numérique de la société qui amène à un développement massif des échanges par voie dématérialisée, mettant en exergue le besoin d'un cyber-espace de confiance à même de garantir la sécurité de ces échanges, en assurant notamment la fiabilité des informations transmises, l'innocuité des services utilisés et plus largement le respect de la vie privée des citoyens."***

Elle repose sur **deux défis majeurs** auxquels les **entreprises** et les **acteurs publics** doivent faire face : la **cybersécurité** et la **conformité** des données à caractère personnel. Elle est d'ailleurs souvent associée à la mise en place d'une **réputation** en ligne fiable, la **crédibilité**, la **transparence** et la **garantie** aux clients d'une expérience solide et sécurisée.

Pour garantir la confiance numérique, l'organisation doit donc mettre en place des **moyens humains et techniques** afin d'assurer la fiabilité de **l'identification**, la **sécurisation** des **flux**, notamment lors des **transactions**, et **l'hébergement** et la **conservation** des données.

… CE QUE LA CONFIANCE NUMÉRIQUE N'EST PAS.

La confiance numérique n'est pas une garantie absolue de sécurité. Même avec les meilleures pratiques et technologies en place, il existe toujours un risque inhérent lorsqu'on confie des informations à des systèmes numériques. L'environnement numérique est une course permanente entre des acteurs ayant des intérêts divergents. L'hostilité se manifeste principalement par la criminalité, la concurrence déloyale et plus généralement par des atteintes.

La confiance numérique n'est pas un blanc-seing, elle n'invite pas l'entreprise, le chef d'entreprise et l'utilisateur final à être complaisant ou négligent en ce qui concerne sa sécurité numérique. Les utilisateurs doivent toujours être proactifs et vigilants. L'entreprise doit encourager les comportements vertueux et montrer l'exemple.

La confiance numérique se distingue aussi du **sentiment de confiance**. L'environnement numérique peut être familier, cela ne signifie pas pour autant que tous les éléments de chaîne, de l'ordinateur, qui peut ne pas être celui utilisé habituellement, à la connexion au site, à la plateforme qui peut présenter des failles.

...LES LIMITES DE LA CONFIANCE NUMÉRIQUE

La confiance numérique dépend fortement de la technologie utilisée, qui est en constante évolution.
Cela signifie que les mesures qui renforcent la confiance numérique aujourd'hui ne peuvent pas être efficaces demain. La confiance numérique repose sur une connexion numérique, des intermédiaires techniques. Il faut donc avoir confiance dans le système technique et les partenaires économiques auxquels ils sont attachés.

Deuxièmement, **la confiance numérique est souvent compromise par des facteurs humains,** de l'erreur humaine à la malveillance interne ou externe, il y a toute une échelle de gravité des atteintes.

Enfin, la confiance numérique est également limitée par des **questions de juridiction et de gouvernance**. Les lois et réglementations varient d'un pays à l'autre, ce qui peut entraîner des incohérences et des incertitudes. L'europe présente ainsi des maturités différentes vis-à-vis des technologies, toutefois, la volonté d'harmoniser les outils et les méthodes est un atout essentiel pour garantir aujourd'hui la confiance numérique.

•••

Réfléchir sur la confiance numérique notamment pour les professions réglementées revient à avoir une approche systématique et s'interroger sur les moyens de :

- **Garantir que la chaîne et les processus d'informations soit traitée de manière sécurisée et confidentielle, qu'il s'agisse de transactions en ligne ou de partage de données, la sécurité des données personnelles et financières et la fiabilité du service sont un impératif que doit garantir autant le professionnel que la plateforme en ligne utilisée.**

- **Assurer la conformité réglementaire en matière de protection des données et de cybersécurité.**

- **D'innover : la confiance numérique peut également favoriser l'innovation et créer un cercle vertueux. Avec une confiance accrue dans les technologies numériques, les entreprises seront plus susceptibles d'adopter de nouvelles technologies et de nouveaux modèles commerciaux.**

03. IMPORTANCE DE LA CONFIANCE NUMÉRIQUE DANS LE MONDE DIGITALISÉ

Depuis plusieurs années, nous évoluons vers un monde de plus en plus incertain et conflictuel et l'élection potentielle de Trump en novembre 2024 ajoute encore un peu plus d'incertitude à cette incertitude.
Les institutions et initiatives (datagouv.fr) comme la CNIL, l'ANSSI, les observatoires comme celui des incidents de sécurité des systèmes d'information pour les secteurs santé, permettent de prendre la mesure du danger. En 2023, la CNIL dans son dernier rapport en a donné quelques chiffres:

- 47.000 appels
- 16433 plaintes
- 81393 DPO nommés / désignés.

Mais l'Europe a une approche qui lui est propre de la confiance numérique et des technologies, distincte des Etats-Unis et de la Chine. L'Europe préfère définir un cadre et innover dans ce cadre, tandis que les USA, préfèrent innover et réguler après. Or dans le domaine de la cybersécurité et l'intelligence artificielle, la diffusion des outils, des pratiques des utilisateurs dans les entreprises se fait de plus en plus rapidement. Chatgpt a ainsi été adopté en moins de trois mois par 200.000 millions d'utilisateurs.
A l'avenir la rencontre des deux technologies et la future l'osmose qui peut naître entre les deux peut être infiniment destructeur pour la confiance numérique. Il est donc important de faire évoluer régulièrement les outils, les méthodes, d'avoir des capteurs pour conserver un niveau de confiance élevé.

La question de la confiance a engendré de nouveaux marchés, le marché de l'assurance notamment, de la certification et formation. Pour le moment, le marché français de l'assurance cyber représente moins de 3% du marché mondial, et à peine plus de 1% de l'assurance des risques d'entreprises en France. En l'espace de cinq ans, la taille du marché français a presque quadruplé.

A côté des assureurs, ce sont aussi des prestataires, comme les courtiers, les réassureurs, les bancassureurs et les GAFAM qui cherchent à se placer sur ce segment.

Pour aller plus loin, la dernière étude de **Xerfi*** apporte un éclairage important.

- https://www.xerfi.com/presentationetude/le-marche-de-la-cyber-assurance_ABF80

04. PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Les défis de la cybersécurité dans la confiance numérique, un écosystème en mutation

Guy Flament, responsable du Campus Aquitaine de l'ANSSI, dans maintes interventions, nous éclaire sur la question des cyberattaques ciblant les PME et sur la manière de développer une culture de la cybersécurité.

En 2023, les statistiques de la Fédération française de la cybersécurité ont montré que les PME étaient les plus touchées par les cyberattaques, avec 330 000 attaques réussies sur 347 000 menées.

La directive européenne NIS2, qui succède à NIS1, devrait être transposée en octobre 2024. NIS1 visait à harmoniser les règles de résilience cyber en Europe, mais n'a pas tout à fait réussi. NIS2 vise à élargir le périmètre de cette directive. Elle concerne toutes les entités qui emploient plus de 50 personnes ou qui réalisent plus de 10 millions de chiffre d'affaires dans les secteurs d'activité visés, un grand nombre d'entreprises seront concernées, selon qu'elles soient essentielles ou importantes.

Il est important de comprendre pourquoi cette directive est nécessaire.

La première raison est l'état de la menace. Il y a 10 ans, seuls les gros opérateurs, comme les gestionnaires de réseau Télécom ou Énergie, étaient concernés. Cette distinction n'est plus d'actualité. Aujourd'hui, TOUT le monde peut être ciblé et attaqué car ces gros opérateurs se sont protégés.

Les attaquants cherchent alors les maillons faibles et passent au crible leur chaîne d'approvisionnement, leurs clients, leurs fournisseurs pour essayer de remonter à leur système d'informations et donc de trouver une porte d'entrée. Il est nécessaire de protéger ces opérateurs et d'étendre ce besoin de protection.

Avec Nis2, il sera obligatoire de déclarer les incidents. Ce qui implique que les entreprises ne pourront plus se permettre de ne pas avoir de politique de sécurité. Elles devront **documenter** leur organisation en matière de sécurité. Il ne suffira plus de **déclarer** simplement sur l'honneur "je suis organisé", il faudra **prouver** cette organisation.

Ce qui est important de savoir, c'est que Nis2 va **imposer** aux organes de direction **d'approuver** ces mesures de gestion des risques qui vont être prises par leur DSI et donc de **superviser** leur mise en œuvre. Il est prévu dans la directive Nis2 que les organes de direction doivent pouvoir **être tenus responsables** en cas de violation de la directive Nis2. Ce n'est pas juste le DSI qui sera responsable. **C'est le dirigeant qui sera tenu comme responsable.**

Autre changement, à toutes les échelles, les entreprises sont en train de gagner en matûrité face au risque cyber. Elles ont nommé des responsables sécurité ou gestion du risque numérique, **toutefois celui-ci n'est jamais membre du comité de direction**. Il n'a jamais accès directement au dirigeant. Or, la responsabilité incombe au dirigeant.

Cette absence de lien est déplorée par tous les spécialistes cyber depuis longtemps. Alors que paradoxalement le numérique est devenu un élément essentiel de pilotage et d'activité des entreprises dans toutes ses disciplines. **Le cyber est déconsidéré en termes de stratégie au sein de l'entreprise**, avec cette obligation il devient pour le dirigeant, une obligation légale dont il doit répondre.

La sanction financière appuie cette responsabilité. Elle n'invite toutefois pas les dirigeants à provisionner cette somme pour payer l'amende, mais à investir dans les mesures de prévention du risque numérique. C'est un outil de pilotage.

Nis2 n’est pas bâti sur un modèle RGPD où la conformité peut être atteinte à moyen terme. Avec Nis2 soit l’entreprise est conforme, soit elle ne l'est pas.

Nis 2 prévoit aussi des délais courts, puisqu’on a entre 24 et 72 heures pour déclarer qu’on a été victime d’un incident. C'est-à-dire 24 H si on soupçonne qu’il y a un problème, une panne. 72 H si c’est une attaque et qu’on a détecté un point d’intrusion et qu’on est en train d’évaluer ce qui se passe. Pendant un mois, c’est-à-dire la période post-incident, un rapport doit être rédigé pour documenter celui-ci et être présenté auprès des autorités.

… Coaxis, un cas d'étude

Coaxis* a été un signal, une alerte. En l'espèce, un des clients de l'entreprise a été compromis par une cyberattaque. Un cybercriminel se fait passer pour un client légitime. Ce type d'attaque était redoutable, car au-delà des conséquences matérielles qui pouvaient être fatales pour l'entreprise, elle minait durablement la confiance et laissait des traces dans l'entreprise dans les relations entre les collaborateurs et partenaires.

Cette étude de cas particulièrement bien documentée est citée en exemple a plus d'un titre tant la résilience de l'entreprise a été remarquable tout au long de la crise, du plan de continuité jusqu'à la résolution de celle-ci.

On peut retenir les éléments suivants :

1. il est donc essentiel d'avoir réfléchi en amont à une politique de sécurité des systèmes d'information,
2. de prévoir les mesures de prévention, les exercices de simulation, la crise, la reprise d'activité, la continuité d'activité.

C'est l'ensemble de ces trois mesures qui seront systématiquement contrôlées.

*https://www.coaxis.com/incident-de-securite/

Pour Guy Flament, le chef d'entreprise doit toujours garder à l'esprit que la vraie urgence, est et demeure la reprise : récupérer les données, reconstruire les systèmes le plus sainement possible et redémarrer les outils applicatifs. C'est un vrai challenge de la gestion de crise. L'écran noir doit se rallumer avec les applicatifs métiers le plus rapidement possible et dans les meilleures conditions.

Pour Guy Flament, à l'heure actuelle, la probabilité qu'une entreprise ne se soit jamais fait attaquer est faible. Soit l'attaque est en cours et elle est encore non détectée, soit l'entreprise ou le dirigeant ne l'ont pas vu.

Et avec Nis2, il ne sera plus possible de mener une politique de l'omerta et / ou de l'autruche, sans démontrer sa bonne foi et les actions menées pour empêcher et limiter les sinistres.

Quand on regarde les chiffres macroéconomiques, la croissance des attaques est extrêmement rapide et véloce. Les pertes de données ont un coût très élevé, elles sont difficiles à anticiper et retrouver l'intégralité des données est rarement envisageable. Il y a forcément un pourcentage incompressible de perte, un deuil qui doit être fait, un peu comme la part du feu et si bien sûr un sentiment d'urgence domine. "Il n'y a pas de miracles".

Enfin au réflexe humain de l'affirmation “Mais je suis assuré”, suite à un sinistre, l’assureur n’est pas en mesure de reconstituer l’intégralité de l’historique de l’entreprise. Comme tous les acteurs, l’assureur tient compte du ratio coût/bénéfice. Un mot clé : sauvegarde.
Derrière, la colère, la stupeur, le trouble, la victime ne doit pas faire oublier l’entrepreneur, le responsable d’entreprise.

A noter : À l'inverse, si le dirigeant n'est pas en capacité de déclarer ses incidents, s’il n’y a pas une politique de sécurité de systèmes d’information et pas de plan de continuité d’activité, l’entreprise sera sanctionnée. C’est pourquoi il est essentiel, capital de garder tous les éléments de preuves techniques et informatiques qui peuvent être contenus dans les logs ou tous les éléments pour constituer le dossier et étayer la plainte .

A retenir :

- **En cas de doute, commencez par utiliser des auto-diagnostics qui sont proposés par les différents services.**
- **Se faire accompagner par un prestataire labellisé ExpertCyber. Lancé par Cybermalveillance.gouv.fr en collaboration avec l’AFNOR (pdf).**
- **Obtenir une ou plusieurs certifications de l’ANSSI.**
- **Regarder si le modèle Zero Trust peut s’appliquer à son entreprise**

O5. Confiance Numérique et intelligence artificielle : un double usage

La CNIL définit l'intelligence artificielle (ou IA) comme un ensemble d'algorithmes entraînés sur de vastes ensembles de données. L'intelligence artificielle n'est pas une technologie à proprement parler mais plutôt un domaine scientifique dans lequel des outils peuvent être classés lorsqu'ils respectent certains critères.

Pour le Parlement européen*, l'intelligence artificielle représente un outil utilisé par une machine afin de «reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité ».

La confiance en l'I.A. interroge la transparence et la compréhension des "boîtes noires". La réglementation, le Développement, confiance, réglementation et certification par des professionnels sont essentiels pour garantir la fiabilité des solutions d'IA.

CNIL.

*https://www.europarl.europa.eu/topics/fr/article/20200827STO85804/intelligence-artificielle-definition-et-utilisation

… L’intelligence artificielle comme outil de confiance numérique

Si il y a un “game changer” dans tous les domaines, c’est bien l’arrivée de l’IA et sa rapide adoption par le grand public. Cette adoption a été si rapide et les apports si révolutionnaires, que le gap entre les individus et par extension les entreprises qui les utilisent ou pas pose une question sur cette adoption ? Avait-on vraiment le choix ? s’est elle faite à marche forcée ? Car la succession des Sommets mondiaux qui jalonnent la fin d’année 2023 et l’année 2024 et l’inquiétude des acteurs pose question. En novembre 2023 un premier Sommet sur la sécurité de l'IA a eu lieu à Bletchley Park en Angleterre, (lieu hautement symbolique où Turing travailla sur Enigma). Séoul les 21 et 22 mai 2024, et Paris en Novembre 2024.

Réunissant 28 pays ce premier sommet a permis la rédaction et la signature d’un texte la “Déclaration de Bletchley*” actant "le besoin urgent de comprendre et gérer collectivement les risques potentiels de l'IA à travers un nouvel effort mondial, visant à garantir que l'IA est développée et déployée de manière sûre et responsable." Texte dont la France est signataire.
Comme le souligne la déclaration de Bletchley, “pour le bien de tous, l’IA doit être conçue, développée, déployée et utilisée de manière sûre, de manière à être centrée sur l’humain, digne de confiance et responsable.”

*https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

Ce rappel aux différents pays signataires, et acteurs, souligne qu'à côté des opportunités qu'ouvre l'IA, de nombreux risques existent aussi au niveau individuel et systémique. « *Parallèlement à ces opportunités, l'IA présente également des risques importants, y compris dans* ***les domaines de la vie quotidienne****. De nombreux risques liés à l'IA sont* ***intrinsèquement de nature internationale "*** *et il est donc préférable de les gérer par la coopération internationale.*

Déjà, la criminalité classique s'est emparée de ces outils pour massifier les attaques cyber sans toutefois atteindre la dangerosité des attaques imaginées dans les années 80-90.
Toutefois les violations de données, les préoccupations concernant la vie privée massive et leur revente sur le darknet ont prouvé la fragilité de nos systèmes d'informations. Il est essentiel de développer des outils et des technologies qui peuvent aider à renforcer la confiance numérique. L'intelligence artificielle (IA) se présente comme un outil puissant dans cette quête. Elle offre des possibilités considérables pour améliorer la sécurité, la transparence et la conformité dans le domaine numérique.

La Chine, les USA, la Turquie, signataires de l'accord seront des voix à écouter. Elizabeth Kelly directrice de l'Institut américain de sécurité de l'intelligence artificielle, chargée d'assurer la direction exécutive, la gestion et la surveillance de l'AI Safety Institute* et de coordonner avec d'autres initiatives politiques et techniques en matière d'IA au sein du ministère du Commerce, du NIST et du gouvernement sera une personnalité importante à suivre.

*https://www.nist.gov/aisi

…. Une approche européenne de l'IA et de la confiance numérique

Avec le RGPD (2016-18) voilà près de dix ans que les instances européennes se sont emparées de la question de la confiance numérique. Avec NIS1 et NIS2, DORA elles ont posé des briques supplémentaires. L'Europe s'engage à réguler l'IA de manière responsable, en tenant compte des risques, de la responsabilité et de l'évolution constante de la technologie.

Jusqu'à maintenant, la diffusion de la réglementation européenne de l'IA à l'échelle mondiale était encore compliquée tant les intérêts entre les pays sont divergents, notamment les questions de traçabilité, d'éthique, de sécurité, de criminalité.

L'Union européenne* (UE) considère que l'intelligence artificielle (IA) va définir le monde dans lequel nous vivons à l'avenir. Consciente que les défis futurs, dont l'IA sera une composante, elle peut être une source d'instabilité. Pour construire une Europe résiliente pour la décennie numérique, les citoyens et les entreprises devraient pouvoir bénéficier des avantages de l'IA tout en se sentant en sécurité et protégés. L'UE vise donc à faire de l'Europe un hub de classe mondiale pour l'IA et à garantir que l'IA est centrée sur l'humain et digne de confiance.

*https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

Deux mots clés, **Excellence et confiance**, l'approche européenne de l'IA repose sur ces deux valeurs. Elle vise à stimuler la recherche et la capacité industrielle tout en garantissant la sécurité et les droits fondamentaux. En avril 2021, la Commission a présenté son "paquet IA", qui comprend sa communication sur la promotion d'une approche européenne de l'IA, une révision du plan coordonné sur l'IA avec les États membres de l'UE), son cadre réglementaire proposé sur l'IA et une évaluation d'impact pertinente.
La Commission et les États membres ont convenu de stimuler l'excellence en IA en unissant leurs forces en matière de politique et d'investissement dans les programmes Horizon Europe* et Digital Europe* pour un montant d'un milliard d'Euros par an.

L'approche de l'UE en matière d'IA vise à créer un cercle vertueux. En développant un cadre réglementaire solide qui profite aux personnes, aux entreprises et aux gouvernements.

*https://www.horizon-europe.gouv.fr/

*https://digital-strategy.ec.europa.eu/fr/activities/digital-programme

O6. Confiance numérique et intelligence collective: le point de vue de Anna Elviro

Renoncer délibérément à « La confiance numérique et l'intelligence collective » pourrait conduire à des conséquences telles que la méfiance numérique et un repli sur soi. En effet, sans confiance dans les outils numériques et dans la coopération, il pourrait y avoir un recul vers des méthodes plus isolées et potentiellement moins efficaces de travail et d'interaction.
Aborder le sujet de la confiance numérique est crucial à mesure que l'IA devient une composante de plus en plus omniprésente dans nos vies mais elle semble encore inconnue et insaisissable. Et l'anxiété face à l'inconnu est un facteur important. Nous pouvons ressentir la peur d'être dépassé, remplacé ou manipulé.

Pour intégrer véritablement l'IA dans nos processus créatifs, il est essentiel de développer un sentiment de sécurité, de fiabilité technologique et de réassurance. Apprivoiser l'IA et démystifier ses capacités et limites peut aider à réduire la peur.
L'IA, sans émotions, ne ressent pas la peur ni d'autres sentiments, ce qui la distingue fondamentalement des êtres humains.

Pour relier efficacement l'IA à l'intelligence collective, il est important de ne pas la laisser dominer ou monopoliser l'espace mais plutôt de lui attribuer une place que nous jugeons appropriée. Adopter une approche ouverte, exploratoire et critique peut permettre de maximiser les avantages tout en minimisant les risques.

...

Expérimenter l'intégration de l'IA comme un participant actif dans des sessions d'intelligence collective pourrait s’avérer très pertinent. Cela contribuerait non seulement à améliorer la résolution de problèmes complexes mais aussi à enrichir le processus créatif avec des perspectives uniques que l'IA peut offrir.

La confiance numérique, lorsqu'elle est bien cultivée, sert effectivement de catalyseur pour amplifier la pertinence et l'efficacité de l'intelligence collective. C'est une exploration qui pourrait révéler des synergies puissantes entre l'humain et la machine.

Anna Elviro fondatrice d'Innov'Sens

Sont intervenus dans ce Livre blanc

David Commarmond

Rédacteur avec plus de 15 ans d'expérience dans le secteur de la technologie au sein de Veille Magazine , il a consacré de nombreuses années à comprendre, sensibiliser, évangéliser sur les problèmes de sécurité et de confidentialité qui se posent dans le monde numérique d'aujourd'hui.

Auteur du livre blanc "La Confiance Numérique et gouvernance digigtale", David explore les défis et les opportunités liés à la création d'un environnement numérique sûr et fiable.

Passionné par les dernières tendances technologiques. Il croit fermement que la confiance numérique est une clé essentielle d'un avenir sûr et responsable.

Jacqueline Sala

Jacqueline Sala, Membre du Collège de l'Académie d'Intelligence Economique, est depuis 1996 fondateur et rédacteur en chef de "VEILLE", le magazine des professionnels de l'information stratégique dédié aux enjeux et impacts croisés de la mondialisation, de la sociologie des organisations et des systèmes d'information.

Dès 1995, elle se dirige vers les métiers du conseil stratégique (IFACE, CCIP en 1996) et crée simultanément Veille magazine. Suit en 2005 le salon professionnel ICC "Innovation, Compétitivité et Connaissance" pour accompagner le développement de l'Intelligence économique.

•••

… Jacqueline Sala

Elle est, par la suite, à l'origine de divers événements professionnels tels SEARCH, REPUTATION DAY, INFLUENCE-DAY et DOCUMATION-MIS. En 2012, elle participe à la création des Data Intelligence Awards et, à partir de 2016, organise le salon du B-to-B Data Intelligence Forum (Intelligence digitale et création de valeur).

Formation

- DESS de Sociologie des organisations et Anthropologie sociale, École des Hautes Études en Sciences Sociales, Paris
- Maitrise en Sciences Sociales & Sociologie, Sorbonne-Paris V

Anna Elviro

Responsable pédagogique du programme Executive Coaching d'organisation HEC, Anna Elviro est coach d'organisation spécialisée dans les paradoxes et les contradictions. Elle invite les professionnels à s'ouvrir à de nouvelles options et à découvrir des pistes d'action concrètes.

Auteur du livre « La boîte à outils de la résolution de problèmes complexes. Dunod »