Plaidoyer

## Face à la désinformation et aux ingérences

# Marquer le réel

ETÉ 2025

Mouvement des Entreprises de France

la villa numeris

## :: remerciements

Merci aux membres de notre groupe de travail pour leur participation et leur contribution, **Bruno Breton**, fondateur de Bloom, **Jean-Frédéric Farny**, directeur général de Aday, **David Lacombled**, président de La villa numeris, et **Estelle Prusker-Deneuville**, Mediacampus Manager, Audencia, et les équipes du MEDEF

Les membres du groupe de travail remercient l'ensemble des personnalités qui ont été auditionnées dans l'élaboration de ce travail :

- **Marc-Antoine Brillant**, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum)
- **Jean-Luc Brossard**, coprésident de la commission Numérique et Innovation du MEDEF, VP Innovation de Stellantis, président du Comité des Constructeurs Français d'Automobiles
- **Emilie Devaux-Trébouvil**, secrétaire générale du SNEP
- **Virginie Fauvel**, coprésidente de la commission Numérique et Innovation du MEDEF, PDG d'Harvest
- **Teddy Furon**, directeur de recherche à l'INRIA
- **Aurélien Hérault**, directeur de l'Innovation de Deezer
- **Ivette Hubackova**, directrice des études du SNEP
- **Alban Ondrejeck**, directeur technique d'Anozrway
- **Ludovic Pouilly**, Institutional & Music Industry Relations, Deezer

Merci à **Arthur Brodmann** pour sa relecture attentive

# Un constat, des convictions

Les phénomènes de désinformation et d'ingérence, sans cesse en progression, sont désormais parfaitement connus et documentés. Pourtant, les démocraties apparaissent encore trop souvent passives et les entreprises à peine concernées.

Il en va du risque informationnel comme de la menace cyber : tant que vous n'êtes pas touché, vous ne vous en prémunissez pas ; quand vous êtes attaqué, il est trop tard. Pourtant, les tensions géopolitiques sur la scène internationale, ainsi que les tensions politiques, économiques et sociales dans la plupart des démocraties, montrent à quel point les entreprises deviennent également une cible des mouvements à l'œuvre. Ainsi, dans le cadre de conflits qui les dépassent, de nombreux cas révèlent que des entreprises doivent faire face à des appels au boycott de la part de consommateurs particulièrement sensibles aux enjeux humanitaires et environnementaux.

Nous sommes engagés dans une véritable course contre la montre. La désinformation est sans doute le premier risque mondial des années à venir, alors que les contenus authentiques ne représenteraient que moins d'une attaque sur trois, et que les craintes sont attisées par l'émergence des solutions d'intelligence artificielle générative.

C'est pourquoi, le MEDEF, fort de sa représentativité et de son engagement, et La villa numeris, à la pointe du combat contre la désinformation, ont constitué un groupe de travail pour montrer l'urgence d'agir dans la lutte contre les risques informationnels et les ingérences.

Il nous importe de frapper les esprits en montrant la réalité des menaces et d'imaginer dès aujourd'hui les points de sortie à même de mobiliser les dirigeants et de partager de bonnes pratiques, en capitalisant sur notre conviction que seul le marquage du réel peut permettre de distinguer les communications de bonne foi des manœuvres dilatoires, en authentifiant les sources, en traçant les contenus et en garantissant leur intégrité.

Matérialiser le danger par la constitution de registres et la mise en œuvre de solutions technologiques s'apparente dès lors à un véritable système immunitaire de l'information. À cet égard, il importera de veiller à réduire le financement des sources d'information toxiques.

En cela, les entreprises doivent s'organiser, en améliorant leur connaissance, en formant leurs salariés - et en premier lieu leurs dirigeants - pour identifier au plus tôt les risques afin de mieux anticiper les crises.

**David Lacombled**
Président de La villa numeris

# L’heure des choix

«Rien n’est permanent sauf le changement», nous dit Héraclite. Le philosophe manifeste là la constance du changement. Il en va des attitudes et des postures, des mots et des images. Portés par le flot de contenus qui irriguent nos écrans et nos quotidiens, nous ne cessons d’être marqués par cette circulation dans les moteurs de recherche et les réseaux sociaux. Une information sera ainsi repartagée à l’envi, diffusée, ajustée, modifiée, rectifiée, tronquée, déguisée pour mieux être véhiculée et reprise. Cette démarche s’inscrit, bien souvent, en faveur des uns et au détriment des autres.

Comme les Etats, les entreprises sont, elles aussi, des cibles de premier plan des ingérences étrangères à travers leurs campagnes de désinformation. Les entreprises ne le savent ou ne veulent le voir que trop peu pour veiller à s’en protéger. Poumon économique des pays dans lesquels elles évoluent, les entreprises se doivent d’affronter une expansion des menaces informationnelles dans un contexte propice aux ingérences et aux manipulations.

Aussi, développer un véritable système immunitaire de l’information est pour les entreprises une manière de s’armer avec l’ambition de se prémunir des menaces. Authentifier les sources, tracer les contenus, garantir leur intégrité : voilà l’ambition du marquage du réel. Lui seul permettra de distinguer communications de bonne foi et manœuvres dilatoires.

Décider de marquer le réel, c’est poser un choix fort face aux contenus créés de toutes pièces à des fins peu honorables de manipulations volontaires à des fins idéologiques ou mercantiles, parfois les deux. Marquer le réel, c’est réaffirmer l’intention première de l’auteur, à condition qu’il soit de confiance, d’un contenu, d’une image ou d’une donnée. Le sceau du marquage sera ainsi garant du contenu d’origine et se détachera des pâles copies ou trahisons façonnées par des solutions d’intelligence artificielle générative, détournées par des individus malveillants, qui ne cessent de s’imposer et de porter à confusion ses lecteurs qui se retrouvent dupés. Pour y parvenir, il sera nécessaire de créer de vastes registres à même de permettre l'authenticité et la traçabilité des œuvres et des contenus.

Forts d’une réflexion ancienne, des auditions et des travaux que nous avons réalisés conjointement nous sommes convaincus que l’entreprise doit se saisir de cet outil porteur de confiance qui sera le plus à même d’alerter et de sensibiliser pour protéger de ces désinformations.

Il est temps pour les entreprises de réaffirmer haut et fort leurs convictions face aux risques nombreux qu’elles encourent. En marquant le réel, elles font un pari à long terme : l’authenticité. C’est bien un enjeu collectif où public, privé et citoyens doivent prendre leur part.

# Des risques à regarder droit dans les yeux

Campagnes de déstabilisation, manipulations et ingérences numériques étrangères noircissent les pages des journaux tant elles sont massives et conséquentes pour nos démocraties. Ces attaques s'inscrivent dans des tensions géopolitiques, économiques et sociales très fortes. Des équipementiers aux constructeurs, toutes les organisations sont concernées et non plus uniquement le voisin que l'on se contente de regarder en seuls spectateurs cachés derrière nos fenêtres. En effet, en décembre 2024, 47% des Français ont déjà été confrontés à une fake news sur la santé, contre 37% en 2020, nous apprend le sondage réalisé par l'institut Vérian pour Harmonie Santé en partenariat avec l'Inserm. Les conséquences sont dramatiques puisque ce sondage indique que 43% ont même agi en se basant sur une information mensongère, contre 32% en 2020[1].

Les entreprises deviennent, pour les mouvements à l'œuvre, une cible géopolitique de choix des campagnes coordonnées de déstabilisation en ligne renforcées par l'hyperpuissance des réseaux sociaux et des contenus – textes et vidéos - multiples qui sont générés de façon artificielle. D'ailleurs, 28% des Français se disent très souvent confrontés à des informations délibérément fausses ou trompeuses sur les réseaux sociaux, contre 17% pour les boucles de discussion sur des messageries en ligne et 11% dans les médias traditionnels (d'après l'étude « L'impact de la désinformation sur les élections européennes 2024 » réalisée par Ipsos et Sopra Steria en février 2024)[2].

On se souvient des campagnes de déstabilisation tenues en amont des Jeux olympiques et paralympiques (JOP). En effet, « sur la période de veille considérée (avril 2023-8 septembre 2024), VIGINUM a identifié 43 manoeuvres informationnelles ayant ciblé les Jeux de Paris 2024, s'appuyant sur différents modes opératoires documentés », relève VIGINUM en présentant un rapport de synthèse sur la menace informationnelle lors des JOP de Paris[3]. Les attaques peuvent être initiées tant par des acteurs étatiques que paraétatiques qui sont d'ailleurs officiellement plus ou moins proches de la France. Ne soyons pas dupes des discours véhiculés.

Il en va de l'avenir de nos entreprises puisque ces manœuvres représentent, pour elles, des risques multiples et particulièrement néfastes. L'image peut être entachée. Avec ces attaques, les auteurs entendent atteindre la réputation de l'entreprise visée au travers des narratifs employés.

[1] Sondage sur les fake news en santé : que disent les Français

[2] Européennes 2024 : les Français particulièrement vulnérables à la désinformation

[3] Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024

Le risque économique est bel et bien là lors d'un appel au boycott émanant de parties prenantes via les réseaux sociaux. En résulte, un chiffre d'affaires qui se voit plombé. La cotation de la société peut, elle aussi, vaciller. Le risque peut également être d'ordre managérial lors d'une déstabilisation interne concernant les ressources humaines ou bien le social, en raison d'un narratif utilisé sciemment pour contrer le bon fonctionnement de l'organisation.

Extrêmement fin. Le niveau d'attaque l'est résolument et, de plus en plus. L'IA et les outils génératifs sont au cœur des différents modes opératoires. Les nouvelles solutions technologiques sont le vecteur de ces attaques. Avec l'IA, il est bien plus facile d'industrialiser la production de contenus non vérifiés et de les diffuser massivement sur les réseaux sociaux. Cela est d'autant plus ennuyeux que la prime n'est plus donnée aux sachants. La désinformation est, bel et bien, un risque quand on sait que l'IA est à l'initiative de nombreux contenus. C'est d'ailleurs un sujet soulevé par l'industrie du disque : le risque de se retrouver avec des produits entièrement générés par l'IA.

Des cibles à part entière. Même si elles ne se sentent pas directement concernées, les entreprises sont l'objet des attaques. En effet, trop souvent, les entreprises tant qu'elles ne sont touchées, ne se prémunissent des menaces. Il est alors trop tard. Certes, quelques grandes entreprises sont à présent sensibilisées et équipées parce qu'elles ont été, par le passé, visées. Il est néanmoins difficile, pour la majorité des entreprises, d'identifier ce sujet comme une menace qui les concerne au premier chef.

Nous déplorons que les campagnes de déstabilisation et de manipulation ne soient pas encore inscrites en haut des agendas des dirigeants qui n'ont que trop faiblement pris conscience de ce risque et ne savent comment l'appréhender. Il n'y a pas de petits profils. Aussi, nous ne pouvons continuer à nous taire et à rester les bras croisés.

---

# La prime à l'authenticité

Appréhendons et décryptons les mouvements à l'œuvre pour nous en prémunir et riposter dans le respect de la loi. Promouvons des solutions opérationnelles de prévention qui conduiront à un standard. Le marquage du réel, nous en sommes convaincus, est l'une des solutions prouvant la véracité et l'origine d'un contenu.

Face aux usages malveillants, protégeons nos contenus. Il est crucial de réapprendre à distinguer le vrai du faux face à toute forme d'ingérence voulant bousculer la sécurité économique d'une entreprise. Ne restons pas passifs. Les entreprises doivent, elles aussi, entrer dans une logique d'influence en engageant une stratégie, notamment sur les réseaux sociaux.

Les solutions de marquage ont pour objet d'immatriculer et de marquer un contenu pour faire en sorte qu'il puisse circuler en partant du principe que les métadonnées peuvent être décrochées d'un document. Effectivement, lorsqu'une image est disséminée sur Internet, elle peut perdre ses métadonnées. Aussi, une technologie de marquage permet de réconcilier un document qui circule avec ses métadonnées. On peut chercher la confrontation avec les métadonnées d'origine et détecter une altération même minime grâce à un système de marquage. D'ailleurs, au début des années 2000, un nombre important de recherches en France ont porté sur le tatouage numérique notamment à Rennes, sujet qui connaît, aujourd'hui un rebond.

Le marquage (watermarking) du réel est garant de la légitimité et de l'authenticité d'un contenu authentique face à un contenu artificiel généré par une intelligence artificielle. Aussi, n'importe qui peut s'assurer grâce à cette solution de l'authenticité d'un document et garantit, tout au long de sa vie, sa non-altération. D'ailleurs, l'IA ne peut générer de marqueur. Un communicant pourra ainsi tracer ses communiqués de presse et s'assurer que personne n'usurpe son identité dans leur diffusion. Dans le cinéma, on retiendra cette solution pour la copyprotection. On l'utilisera pour s'assurer de la trajectoire d'une image de presse dans le cadre du droit d'auteur et des droits voisins. Initiative à relever : Viginum et le pôle d'expertise de la régulation numérique (PERen) ont, avec un projet d'infrastructure, « développé les briques logicielles d'une interface standardisée open source » afin de « savoir à quel détecteur se fier en fonction du contenu testé ». Une approche opérationnelle et collaborative – avec une interaction qui offre un gain d'efficacité.
De la télévision à la radio en passant par le cinéma, quand nous consommons des médias, nous sommes, sans le savoir, exposés à un contenu tatoué. Il importe de structurer la stratégie choisie en instaurant des solutions technologiques labellisées de marquage et de traçabilité. Se doter d'un système robuste aux attaques est essentiel afin d'effectuer des vérifications très rapidement et efficacement. Une solution de marquage du réel peut apporter une caution de vérification indépendante comme peut le faire une agence d'Etat.

Pour autant, il convient de lever plusieurs freins pour s'assurer d'une bonne mise en œuvre du marquage du réel.

Le coût est soulevé par plusieurs parties prenantes. Recourir à une solution de marquage nécessite des investissements tant en infrastructure qu'en réseau. La technologie doit aussi être adaptée. Or, peu assument la responsabilité du financement du dispositif au regard de la complexité de celui-ci. Les PME ont souvent des moyens limités pour se saisir du sujet.

Le sujet est complexe – notamment sur le plan juridique et réglementaire. Il s'agit de s'assurer d'une bonne compréhension, sensibilisation et adoption. Aussi, en intégrant une solution de marquage, veillons à ce qu'elle n'exclue pas des publics qui la considèrent comme inaccessible et ont l'impression d'être démunis. Autre point d'attention : le mécanisme d'interopérabilité entre les technologies de marquage.

Comme le marquage est imperceptible, on ne sait qui a effectué le marquage ni par quel algorithme. Il n'y a pas encore de standard mais uniquement des solutions propriétaires. Se pose la question de la sécurité du tatouage. Enfin, le marquage offre une garantie théorique avec une chance sur un million, d'avoir un faux positif. Elle peut se réduire à une sur un milliard avec un risque toutefois que le système soit alors moins robuste. Ce sont là, autant de points à éclaircir pour confirmer l'usage de ces solutions essentielles pour garantir la confiance dans l'information et les échanges au sein de l'entreprise et vis-à-vis des audiences externes. Aussi, il importe d'organiser dès l'amont cet investissement pour que l'entreprise puisse protéger ses propres actifs.

# Jouons collectif

Dirigeants, préparez-vous dès à présent. Il en va de vos responsabilités de repérer, de convaincre et d'expliquer tout le rôle que recouvre le marquage du réel. Vous êtes directement concernés. Comment être certain de l'authenticité d'un document qui y est diffusé ? Il convient de disposer d'une stratégie formelle et d'embarquer les membres des comités exécutifs des entreprises face à cette désinformation de plus en plus prégnante.

Les collaborateurs doivent, eux aussi, être pleinement mobilisés. Il est nécessaire de les former rapidement en les sensibilisant aux risques. Cela peut prendre la forme d'investissements dans des outils de prévention et de protection mais aussi de la formation continue pour appréhender au mieux et dès l'amont ces campagnes. Des ressources pédagogiques associant bonnes pratiques et conseils peuvent être proposées pour armer les salariés. Instaurons, dans nos entreprises, une vraie culture de la sécurité de l'information comme elle existe dans les armées et également au sein des entreprises outre-Atlantique. Aussi, tout émetteur et tout récepteur d'information dans des entreprises en B2B qui communiquent se doit d'y être particulièrement vigilant en mettant en exergue dans des campagnes de sensibilisation facilement accessibles pour les collaborateurs.

Embarquons aussi la jeune génération pour créer un réflexe qui s'avérera salutaire : vérifier immédiatement un contenu. En effet, « les plus jeunes ont plus souvent le sentiment d'être confrontés à de fausses informations » relate l'étude Ipsos pour Sopra Steria « L'impact de la désinformation sur les élections européennes 2024 » : 81% des moins de 35 ans se disent en effet souvent confrontés à des informations délibérément fausses ou trompeuses sur les réseaux

sociaux[4]. Afin d'encercler la désinformation et de déceler les fausses informations, la pédagogie est clé. Aussi, le ministère des Armées donne des clés pour « reconnaître une image générée par une IA » dans un guide contre la désinformation publié en juillet 2024[5]. Dès le collège, il est important de sensibiliser les adolescents et de les inciter à cultiver un regard critique face aux manipulations de l'information. N'oublions pas également le rôle joué par les formateurs en les sensibilisant également et en leur donnant les outils nécessaires.

Pour créer un véritable écosystème de confiance, la coopération entre parties prenantes est cruciale. Au sein des entreprises, plusieurs postes sont de véritables pivots. Un directeur de la sécurité, de la communication ou encore de la cybersécurité sont des rouages essentiels. Il est important de veiller à l'actualisation et à la mise à jour des outils. Dans la guerre informationnelle que nous traversons, la communication de crise est clé. Le sujet du marquage du réel est bien un sujet transverse et polymorphe qui requiert des experts pour le risque. Veillons à ne pas tout catégoriser et figer dans la technique et à bien inclure l'analyse et le décryptage dans les approches que nous adoptons. Aussi, il importe d'ajuster ou de repenser les organisations des entreprises pour les adapter au mieux aux menaces.

Acteurs publics et acteurs privés doivent travailler et coopérer à l'échelle nationale comme européenne. Il est essentiel que l'Etat y prenne, lui aussi, sa place et bien au-delà des seules périodes d'élections pour s'assurer du bon fonctionnement de celles-ci dans un contexte de guerre informationnelle. En effet, bien des démocraties apparaissent en second plan en ne se positionnant pas fermement face aux menaces de désinformation. L'enjeu des registres est un exemple significatif de cette nécessaire coopération. Ce sujet nous concerne tous pour affronter les manœuvres informationnelles. Aussi, il importe d'interroger et d'interconnecter les registres entre eux. Le standard des données des registres doit être un point d'attention.

Un système de standardisation qui prend en charge tant l'interrogation que l'interconnexion serait très précieux. Il prendrait la forme d'une instance référente qui indiquerait quels sont les registres de même nature ou bien leurs équivalents. Sortons enfin des silos qui nous enferment. Prenons appui sur les structures organisant la sensibilisation des entreprises. Participons aux appels à projet en associant nos forces pour prendre à bras le corps ce sujet fort d'un partenariat public-privé affirmé.

Dès lors, décidons de structurer la question du marquage du réel à l'échelle internationale. L'impulsion doit être portée au niveau européen en matière de politique en étant attentif à éviter toute difficulté liée à la pré-transposition ou encore à la surtransposition que nous ne connaissons que trop bien ici. Pour cela, mettons de côté des consortiums qui diffèrent d'un pays à l'autre.

Les entreprises doivent s'échanger leurs bonnes pratiques. Un témoignage d'un de

[4] Européennes 2024 : les Français particulièrement vulnérables à la désinformation

[5] Guide contre la désinformation 2024

nos pairs est celui qui sera, bien entendu, le plus écouté. Parce qu'il a le même niveau de responsabilité, parce qu'il est dans un secteur similaire, nous le considérons comme plus légitime. Nous sommes convaincus de la force du témoignage. Revenir sur une campagne de déstabilisation, mettre en perspective les actions menées face à des manipulations opérées sur le numérique. Un message doit être véhiculé : cela n'arrive pas qu'aux autres. Veillons à ne pas nous cacher mais bien à partager les leçons tirées. ❐

---

# La villa numeris
## //. unlock the future, make it human

La villa numeris est un think tank indépendant qui promeut un modèle européen et ouvert du digital affirmant la primauté de l'humain

**Notre mission :** permettre aux décideurs de comprendre et d'anticiper les transformations sociétales et économiques, d'agir en conséquence, de sensibiliser et de mobiliser pour donner du sens aux organisations et réussir leur mutation.

La villa numeris est une association de Loi 1901 présidée par David Lacombled

### Nos travaux :

**:: Une approche généraliste sur de grandes thématiques :** IA, data, tech, fabrique de l'opinion, nouvelles formes de travail, santé, territoires connectés

**:: Des rencontres exclusives :** 3 cycles de rencontres exigeants et conviviaux avec des dirigeants, acteurs de la révolution digitale : les tendances du marché, les enjeux citoyens et la géostratégie

**:: Une plateforme dédiée :** centre de ressources, de services et de partage

**:: Des opérations spéciales et exclusives :** assises de la Data transformation en janvier à Bercy, Observatoire de la Souveraineté numérique

la vi//a .
numeris

*unlock the future, make it human**

hello@lavillanumeris.com
+33 7 80 96 11 11
http://www.lavillanumeris.com

**libérez l'avenir, rendez-le plus humain*