



MINISTÈRE DE L'ÉDUCATION NATIONALE

*Liberté
Égalité
Fraternité*

Décrypter le numérique, transformer l'enseignement - Cahiers thématiques



Surveillances

N°29

Octobre 2026



Cette nouvelle édition thématique des Cahiers ÉduNum sur le numérique pour l'éducation explore la notion de *surveillance* à travers les réflexions stimulantes apportées par le monde universitaire mais aussi les différents éclairages didactiques et pédagogiques proposés par le groupe national d'experts du premier et du second degré avec l'appui de l'inspection générale de l'éducation, du sport et de la recherche (IGÉSR). Deux grandes parties rythment ainsi ce document collaboratif.

Dans une première, **Olivier Aïm**, enseignant-chercheur à Sorbonne Université (CELSA) en théories des médias, spécialiste des sujets surveillanciers, s'est prêté à l'exercice d'un entretien à distance structuré en quatre questions-réponses visant à clarifier le champ sémantique tout particulièrement prolifique de la surveillance. L'une des formes analysées au sein de ce dossier est celle de *sousveillance*, abordée en particulier dans les travaux de **Jean-Paul Fourmentraux**, professeur des universités, au sein d'Aix-Marseille Université, dont les recherches interdisciplinaires portent sur les enjeux politiques et anthropologiques des arts et des technologies contemporaines. Enfin, le troisième axe de réflexion expose le projet de thèse du designer **Geoffrey Dorne** qui s'inscrit à l'intersection des sciences de l'information et de la communication, des études sur la surveillance et du design graphique, en examinant les stratégies de camouflage civils et militaires face aux drones sur les territoires en guerre, une approche combinant analyse des dispositifs technologiques, OSINT, ethnographie par le design et étude desdites stratégies de camouflage en zones de guerre.

La seconde partie offre comme à l'accoutumée des perspectives disciplinaires ancrées dans des pratiques de terrain. Chaque discipline ou enseignement présente un point de vue singulier en se référant aux programmes scolaires et aux expérimentations réelles menées dans les académies, indexées pour la plupart dans le réservoir national Édubase (scénarios pédagogiques identifiés par le logo  Édubase au sein de ce dossier). La notion de surveillance s'applique à la prévention des risques naturels et au suivi de la biodiversité, aux réalités du monde professionnel où elle interroge les méthodes de contrôle au travail, et suscite par ailleurs des débats sociétaux sur l'équilibre entre sécurité publique, protection des données personnelles et libertés individuelles. Cette réalité contemporaine trouve un écho puissant dans la littérature surveillancière, où les fictions dystopiques et essais critiques ont, depuis des décennies, anticipé et disséqué les mécanismes d'un monde connecté sous observation permanente.

L'approche pédagogique pluridisciplinaire se concentre principalement dans ce dossier sur cinq champs : les **arts plastiques** explorent comment la surveillance est dénoncée, détournée ou subvertie dans le champ artistique ; l'**éducation aux médias et à l'information** (EMI) décrypte les conflictualités informationnelles contemporaines, et les méthodologies d'enquête et de vérification de l'information ; la **philosophie** se penche quant à elle sur la vision par ordinateur et les réseaux de neurones convolutifs et propose dans un second temps de repenser la surveillance en optant pour une éthique de la relation ; enfin, les **sciences économiques et sociales** abordent la surveillance numérique au travail tandis que les **sciences techniques et industrielles** analysent la surveillance des infrastructures de l'information à l'aune des cybermenaces protéiformes.

Sommaire



Matthew Henry, *Surveillance bricks* Free Stock Image. Image recadrée, StockSnap, CC0 1.0

4

Théories de la surveillance

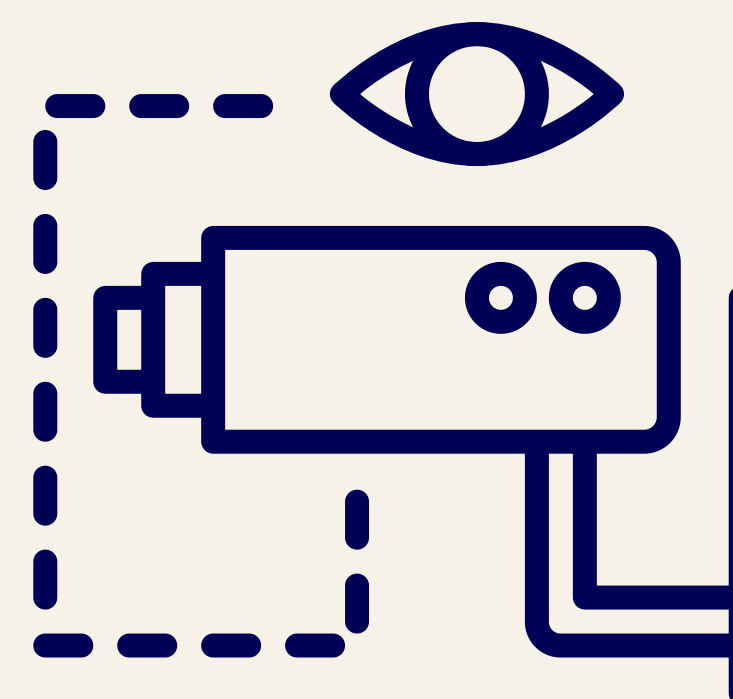
Quatre questions à Olivier Aïm



9

Arts et sousveillance

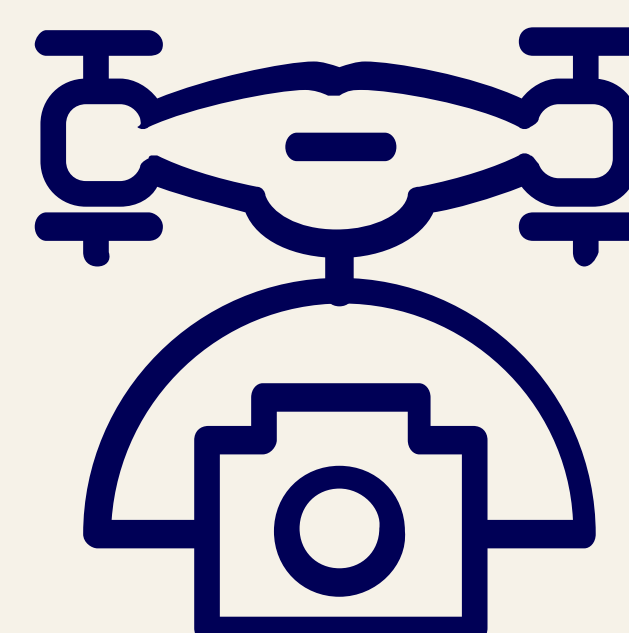
La notion de sousveillance
chez Jean-Paul Fourmentraux



14

Dronisation de la surveillance

Geoffrey Dorne : surveillance,
camouflage et design graphique



19

Pédagogie

Arts plastiques, éducation
aux médias et à l'information,
philosophie, sciences économiques
et sociales, sciences et techniques
industrielles

80

Bibliographie

4 Théories de la surveillance



© Olivier Aïm. Avec l'aimable autorisation de l'auteur.

Olivier Aïm est chercheur à Sorbonne Université (CELSA) où il enseigne la théorie des médias. Il s'est spécialisé depuis une quinzaine d'années sur la question de la surveillance et a publié en 2020 le premier ouvrage en France consacrée aux théories surveillanciennes (Les Théories de la surveillance. Du panoptique aux Surveillance Studies, Armand Colin, collection "U"). Il a consacré de nombreux articles sur le sujet et coordonné depuis plusieurs numéros de revues (Quaderni, Etudes digitales, etc.) afin d'observer les évolutions techniques, politiques, sociales, mais aussi culturelles de la surveillance.

Entretien avec Olivier Aïm : théories de la surveillance

🔗 *Le terme de « surveillance » est utilisé comme matrice conceptuelle : dans quelle mesure ce terme-parapluie est-il suffisant pour décrire l'ensemble des phénomènes de contrôle social ? Doit-il être complété par d'autres notions ?*

Pour commencer, il importe de noter que, du point de vue académique, l'étude de la surveillance s'est développée depuis trente ans au sein d'un champ de recherche appelé *Surveillance studies*. Ce champ s'est structuré de manière très rapide au sein des universités anglo-saxonnes puis européennes, et doit sans aucun doute son succès à l'essor des nouvelles technologies, notamment numériques, qui ont rendu visibles les logiques de collecte de données au sein de nos vies de plus en plus connectées. En ce sens, on pourrait dire que ce qu'on appelle aujourd'hui « surveillance » d'un point de vue conceptuel équivaut à ce que les fondateurs de ce champ de recherche (**David Lyon** et **Gary T. Marx**) ont nommé dès 2002 la « nouvelle surveillance » et qui reprend elle-même ce qui a été décrit dès le milieu des années 1980 sous le nom de « dataveillance » par le chercheur **Roger Clarke**.

De fait, l'importance des enjeux numériques de la surveillance procède, depuis lors, de la diversification des régimes, des dispositifs et des visées de la captation des données, qui ne sont plus seulement politiques, mais encore économiques, sociaux et culturels. De sorte que la montée en puissance de la notion s'accompagne d'un processus d'autonomisation de ce champ de connaissance, et que le contrôle social n'est plus le seul objectif identifié de la surveillance, mais se doit d'être complété par les questions du travail, de la consommation, du divertissement, de l'école, de la vie familiale et de l'ensemble des pratiques culturelles au sens large. En trente ans, le champ des études surveillanciennes est ainsi passé d'un paradigme dominant les années 1970 et hérité de **Michel Foucault** – celui de la « société de surveillance » – à un double paradigme complémentaire, celui du « capitalisme surveillanciel » (**Shoshana Zuboff**, 2019) et celui de la « culture de la surveillance » (David Lyon, 2018).

Se détachant de la seule dimension politique, ce champ d'études s'est lui-même émancipé en termes descriptifs et a gagné en ampleur analytique. Il en ressort que, du côté de la recherche, tout un travail est en marche pour redéfinir les périmètres et les domaines de la surveillance. En fonction de quoi les notions s'affinent et se complètent les unes les autres : le contrôle, la capture, l'espionnage, le renseignement, l'observation, le suivi, la sécurité, etc. composent une mosaïque de questionnements qui se recoupent sur certains points et se distinguent nettement sur d'autres.

5 Théories de la surveillance

🔍 *L'inflation lexicale autour du radical -veillance (sousveillance, überveillance, distriveillance, etc.) relève-t-elle selon vous d'une véritable productivité théorique, ou d'un pur effet rhétorique qui disperse le champ sémantique sans le clarifier ?*

Comme on vient de le voir, la surveillance s'inscrit dans un champ qui connaît des logiques d'extension et de spécialisations multiples. Ce processus d'extension a avant tout partie liée avec l'évolution historique des technologies de la collecte et de l'exploitation des informations, et notamment des traces numériques. En ce sens, l'émergence de la « nouvelle surveillance » est indexée à l'installation et à la sophistication des outils tour à tour informatiques, numériques et algorithmiques. Sans compter ceux de l'IA qui commencent à innover, en profondeur, les dispositifs de calcul, de traçage et de reconnaissance des données.

Sur un plan macro-politique, ces évolutions sont elles-mêmes mises en relation avec les grands processus de la globalisation, à commencer par les crises ou les grands événements planétaires (on peut penser au Covid ou aux grands rassemblements comme les méga-événements sportifs, par exemple). Soit autant de phénomènes qui accompagnent l'essor des technologies de surveillance.

De ces deux contextes, découle une tentation très forte pour les analystes de la surveillance – qu'ils soient chercheurs, journalistes ou militants – de produire une description de la surveillance déterminée par ses seules innovations techniques (comme l'avait fait le concept de « dataveillance » évoqué plus haut). De là provient sans doute cette passion un peu « panique » pour la production de nouveaux concepts qui cherchent à circonscrire les nouveaux contours de la « société de surveillance » : « omniveillance », « sousveillance », « shareveillance », « équiveillance », etc. Cette propension à la néologie est elle-même nourrie par un modèle qui continue à aimanter le champ, puisqu'il en constitue l'origine théorique : le fameux « panoptisme » de Michel Foucault, construit à partir du modèle d'enfermement connu sous le nom de « *panopticon* » de **Jeremy Bentham**. Là encore, en fonction des évolutions techno-politiques, les observateurs de la surveillance s'emploient à produire des nouveaux modèles panoptiques : « synopticon », « cryptopticon », « banopticon », et plus récemment « technoptique » ou « coronoptique », pour ne citer que les plus connus. Si ces créations lexicales peuvent avoir une certaine valeur heuristique, elles prennent le risque de favoriser ce que Gary T. Marx nomme une « tapisserie conceptuelle » à la fois vivifiante pour le champ qui reflète ainsi ses transformations et son actualité, mais aussi limitante d'un point de vue analytique et épistémologique. Cette inflation lexicale court finalement à chaque fois derrière un modèle unique et totalisant de la surveillance, qui ne peut être que réducteur au regard de la diversité des champs et des pratiques.

La meilleure approche consiste, selon moi, à prendre acte qu'il n'est plus véritablement possible de parler de « la » surveillance au singulier, mais que nous sommes entrés dans l'ère « des » surveillances au pluriel. Ce qui en rend, d'ailleurs, d'autant plus passionnante l'étude, pour complexe qu'elle soit devenue.

6 Théories de la surveillance

🔗 Peut-on encore concevoir des régimes de visibilité non-surveillants, ou toute visibilité devient-elle ipso facto captée par un dispositif de pouvoir ?

Répondre à cette question implique de revenir sur quatre éléments de contexte. Tout d'abord, il convient de rappeler que la question de la visibilité trouve son origine dans *Surveiller et punir* avec le paradigme foucaldien de « l'économie politique de la visibilité ». Pour Foucault, le pouvoir est, en effet, indissociable de la capacité à rendre visible ou non une situation, un individu ou une catégorie d'individus. Le fait est que l'histoire lui a donné raison sur ce point, dans la mesure où la visibilité est devenue la question cardinale en termes d'expression, de médiation, de représentation et, plus largement encore, d'accès au débat public : « visibilité », « invisibilité » ou « invisibilisation » sont devenues les coordonnées premières de l'action politique, citoyenne et militante contemporaine.

Deuxièmement, ce que nous montre l'essor des nouvelles technologies de l'information et de la communication, c'est que la visibilité n'est plus seulement visuelle, mais numérique, sensorielle, indicielle : à l'heure des algorithmes et de l'IA, la visibilité relève avant tout de la traçabilité.

Troisièmement, et pour reprendre ce que nous avons dit plus haut, la surveillance est devenue un objet complexe et pluriel, non seulement dans ses enjeux et ses dispositifs, mais encore dans ses « agencements » et, donc, dans les agentivités (ou « *agency* » en anglais) qui les traversent. La visibilité comme pouvoir est travaillée par des logiques de participation ou de partage. Surveillance et contre-surveillance constituent les termes d'une nouvelle dialectique au cœur de la praxis politique actuelle qui atteste que la « visibilité », au sens de traçabilité, se vit de plus en plus comme un enjeu de conflictualité, tantôt recherché, tantôt contesté. Tout ceci fait que les performances de visibilité sont devenues capitales dans nos vies sociales et dans nos vies de citoyen. Loin de s'estomper ou de se diluer, l'usage surveillanciel de la visibilité se trouve démultiplié, nécessitant d'être toujours plus anticipé, au point que l'on peut parler de « surveillabilité » pour évoquer le régime médiatique et politique qui domine nos sociétés présentes.



© Chappatte - www.chappatte.com. [L'ère de la surveillance](#). Avec la gracieuse autorisation de l'auteur

Quatrièmement – ce point découlant directement du précédent –, la surveillance procède d'une culture, au sens large de ce terme. Tout autant rejetée que convoitée, la surveillance relève autant d'une contrainte, d'une injonction que d'un désir : équipé de ses appareils numériques ou de ses *smart technologies*, chacun « revendique » désormais, comme dirait **Walter Benjamin**, son droit à la visibilité, c'est-à-dire à la transparence et à la surveillance.

7 Théories de la surveillance

🔗 *Comment enseigner une « culture de la surveillance » sans la réduire à une simple critique des dispositifs techniques ?*

Pour résumer ce qui vient d'être dit ici, on peut considérer que la surveillance est devenue, au terme de plusieurs tournants épistémologiques importants, l'objet d'une analyse de plus en plus culturelle. Ce déplacement est massif dans ses effets car il permet dorénavant de distinguer entre une définition restreinte, celle de la surveillance comme contrôle, voire comme espionnage, et une définition élargie, celle de la surveillance comme environnement à la fois social, économique et symbolique.

Enseigner la culture de la surveillance implique un effort de réflexivité consistant à prendre en considération à la fois les dispositifs qui nous contraignent dans nos usages (que ce soit dans les dispositifs urbains que dans le design de nos interfaces, par exemple), mais également ceux qui nous accompagnent quotidiennement dans nos pratiques et nos représentations. Il s'agit ainsi de considérer que la surveillance n'est pas abstraite ou conceptuelle, mais qu'elle est vécue quotidiennement, au sens où elle est tour à tour subie, négociée, agie ou même performée dans nos pratiques numériques les plus banales (le *following*, le *monitoring*, le *watching*, le *screening*, le *checking*, le *stalking*, etc.).



© Raffard-Roussel. [Cage de Faraday de trottinette](#). Avec l'aimable et gracieuse autorisation du collectif : « nous avons fabriqué une cage de Faraday qui empêche les trottinettes d'émettre et de recevoir des signaux électromagnétiques. En supprimant ces signaux, le véhicule ne peut plus être géo-localisé. La cage de Faraday permet ainsi d'exposer un « objet connecté » dans l'espace d'une galerie en l'extrayant momentanément de son réseau de surveillance.

Comme la liste des termes que nous venons de citer l'indique, la surveillance vécue renvoie ainsi aux écrans et à l'ensemble des gestes qui régissent notre vision du monde et notre saisie de notre environnement social, physique et numérique à travers les visées suivantes : reprendre le contrôle de ses informations, gérer sa visibilité et son image, suivre ses données, documenter sa vie, etc. En ce sens, l'éducation à la surveillance comme culture rejoint l'éducation plus générale aux médias, à l'information et donc aux écrans. Non pour prolonger *ad libitum* une critique des dispositifs en soi, mais pour mettre en discussion et perspective éthique notre propre rapport aux images et aux désirs de surveillance. Et donc à la place que nous accordons à l'autre et à nous-mêmes comme objet ou sujet de la surveillance (ainsi que le montreraient, par exemple, les pratiques renouvelées du « *quantified self* »).





© Jean Paul Fourmentraux. Avec l'aimable autorisation de l'auteur.

Jean Paul Fourmentraux, est philosophe et socio-anthropologue (PhD), critique d'art et théoricien des médias français (AICA), spécialisé dans la question du rapport entre art, politique et technologies numériques. Il est professeur à l'Université d'Aix-Marseille, chercheur au Centre Norbert-Elias (UMR CNRS 8562), auteur de plusieurs ouvrages sur les (contre-)cultures numériques, dont *Art et Internet* (CNRS éd., 2010), *L'œuvre Virale : Net art et culture Hacker* (La lettre volée, 2013), *Identités numériques* (CNRS éd. 2015), *Digital Stories* (Hermann, 2016), *Images Interactives* (La Lettre Volée, 2017), *antiDATA : la désobéissance numérique* (Presses du réel, 2020), *Sousveillance. L'œil du contre-pouvoir* (Presses du réel, 2023), « Jean-Paul Fourmentraux » [en ligne] [Wikipédia](#).

Jean-Paul Fourmentraux définit la *sousveillance* non pas comme une simple « vigilance » partagée (qui pourrait glisser vers la délation), mais comme un acte politique et artistique de résistance face à la prolifération des technologies de contrôle de plus en plus intrusives. Le terme synonyme d'*équivveillance* est également employé par l'auteur pour qualifier cette forme de -veillance.

Un panopticon inversé

Selon Jean-Paul Fourmentraux, qui s'appuie sur les travaux de l'ingénieur canadien **Steve Mann**, la sousveillance¹ signifie littéralement « surveiller par le bas » (*watching from below*). Il la distingue de deux autres formes de surveillance en particulier :

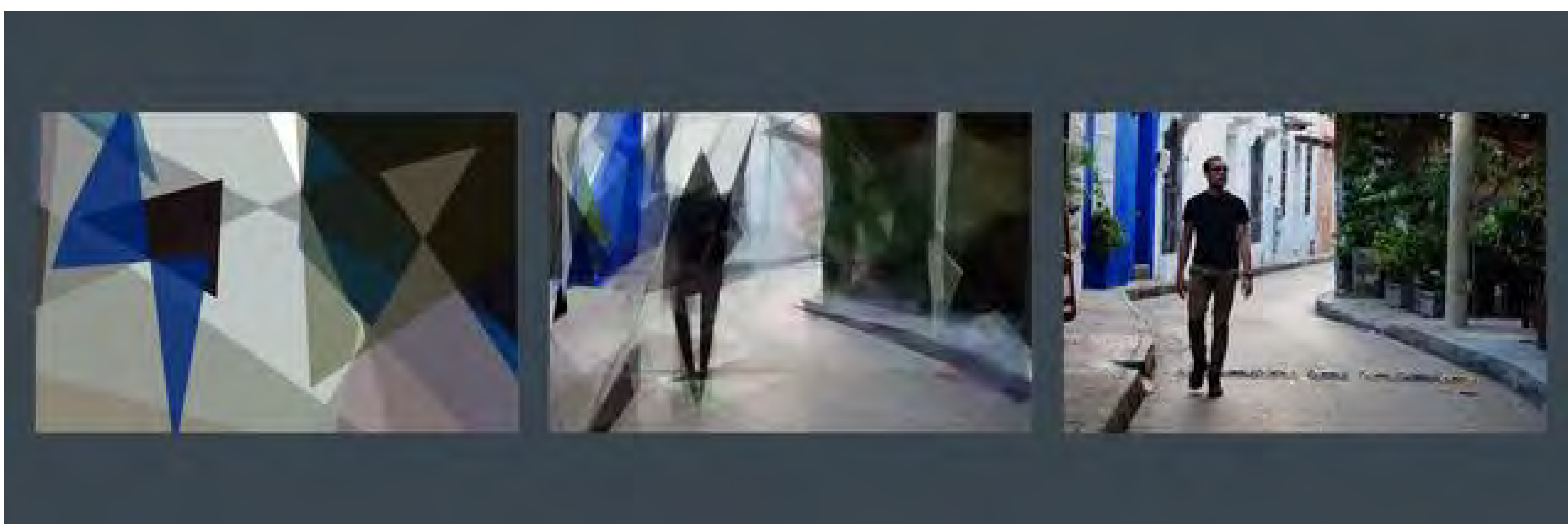
- la *surveillance* (par le haut) exercée par l'État ou les instances de pouvoir ;
- la *vigilance* (au sens d'*autosurveillance* telle que l'évoque **Vanessa Codaccioni**) ou *distriveillance* (en anglais *shareveillance*, telle qu'exposée par **Claire Birchall**), à savoir une *entre-surveillance* distribuée, horizontale, parmi les citoyens, souvent encouragée par les dispositifs sécuritaires et perçue comme un piège de la servitude volontaire.

La sousveillance constitue donc ainsi un panoptique inversé : alors que les logiques de pouvoir cherchent à imposer une transparence totale aux (in)dividus tout en cultivant leur propre opacité, la sousveillance vise à éclairer les actions du pouvoir et à retourner l'œil technologique contre les surveillants eux-mêmes, une forme de contre-surveillance. Le socio-anthropologue attribue à cette notion deux dimensions claires :

- réflexive, voire réflexionniste : elle documente et tend un miroir à la surveillance ;
- opératoire : elle invente des outils de détournement et des contre-feux pragmatiques.

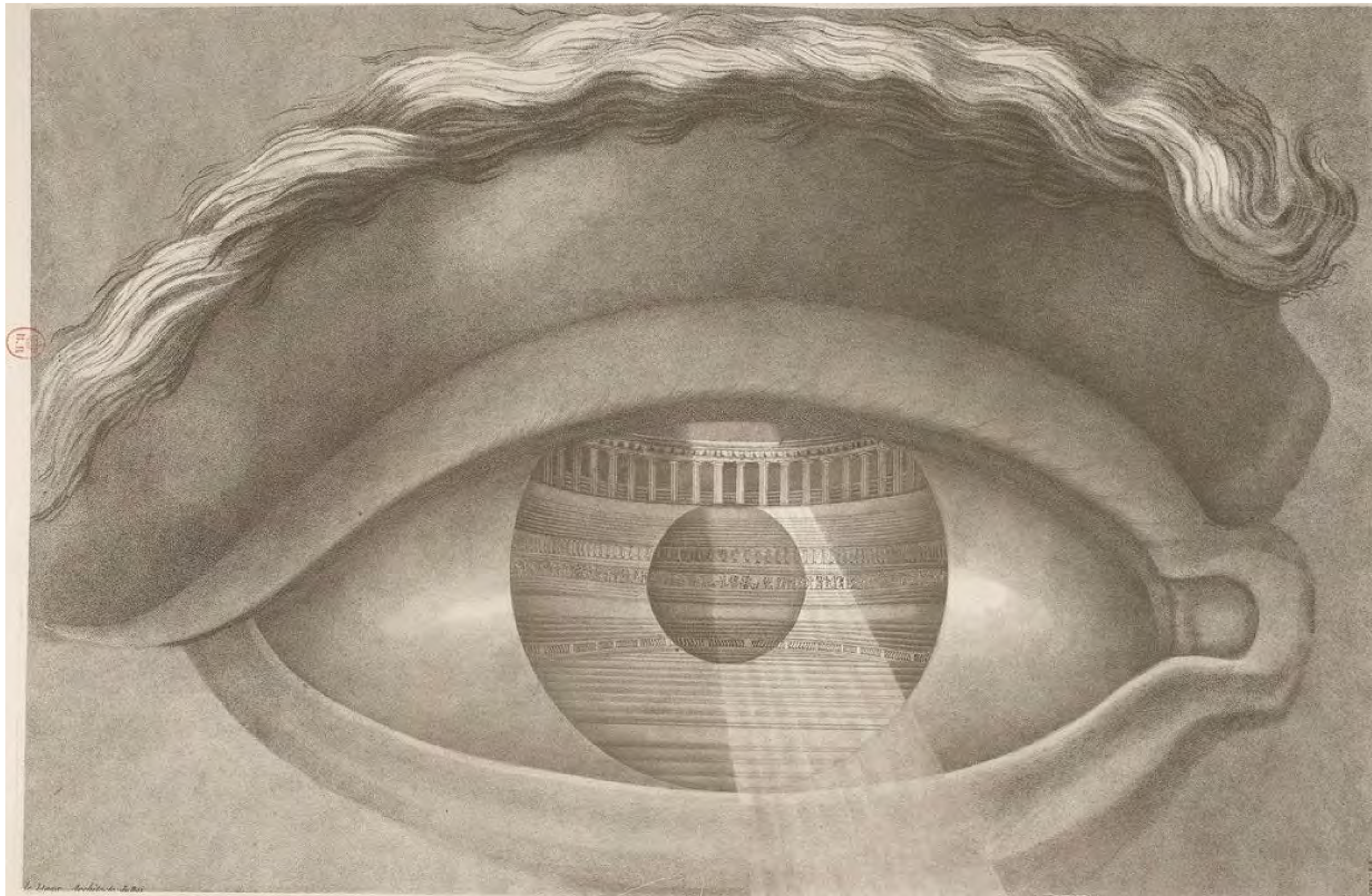
Dans cette perspective, l'art joue un « rôle singulier » permettant d'une part « d'exercer un contrôle social sur ceux qui nous surveillent en documentant leurs politiques et dispositifs de surveillance » et d'autre part « de détourner ces technologies de surveillance et d'opérer leur re-médiation en instruments de contre-observation ».

¹ Fourmentraux, J.-P. (2023). *Sousveillance: L'œil du contre-pouvoir*. Les Presses du réel. p.36



Tactiques de « contre-visualités »

L'auteur convoque une riche série d'œuvres artistiques diversifiées qui illustrent différentes tactiques technocritiques permettant de « ruser avec l'œil du pouvoir » :



Claude-Nicolas Ledoux. « [L'œil réfléchissant le théâtre de Besançon](#) ». *L'architecture considérée sous le rapport des arts, des mœurs et de la législation*, 1804, planche n°113. Source [gallica.bnf.fr/Bibliothèque nationale de France](http://gallica.bnf.fr/Bibliothèque_nationale_de_France)

Paolo Cirio, [artiste conceptuel](#) et activiste italien, s'emploie à utiliser le codage, la fouille de données, les outils d'intelligence artificielle et de réseautage social, non seulement pour en révéler les dérives, mais aussi pour les exploiter de manière tactique, en tant qu'outils de contre-discours, de contre-surveillance et de lutte contre les discriminations. **Trevor Paglen**, artiste multidisciplinaire, géographe et auteur américain, utilise quant à lui des téléobjectifs et des télescopes pour [photographier l'invisible](#) : bases secrètes, câbles sous-marins ou stations d'écoute. Son travail rend tangible l'infrastructure physique et occulte de la surveillance de masse.

Ces démarches « hacktivistes » de contre-surveillance frontale sont complétées par d'autres opérations centrées sur le camouflage et l'obfuscation visant à se rendre invisibles. Ainsi les artistes **Adam Harvey** ([CV Dazzle](#)) , **Zach Blas** ([Facial Weaponization Suite](#)) et **Metahaven** (*Wikileaks scarf*) développent différentes méthodes pour tromper les algorithmes de reconnaissance faciale. Harvey utilise le maquillage et la coiffure, tandis que Blas crée des masques amorphes qui agrègent des données de visages pour devenir indétectables. **Hito Steyerl** ([How Not to be Seen](#)), cinéaste, écrivaine et artiste visuelle allemande, dont il faut rappeler le rôle d'assistante-réalisatrice et directrice technique pour **Wim Wenders** sur *Jusqu'au bout du monde*, propose au sein d'un manuel vidéo structuré en cinq chapitres des « leçons » ironiques pour échapper à la détection et l'enregistrement par les caméras. **Rémi Lauvin** indique² : « Si, aujourd'hui, le *deepfake* remet en cause de façon radicale certains paradigmes qui associent l'image filmée à la captation du réel, le film de Steyerl suggère déjà que l'image peut être, également concernée par le réel et par sa falsification ». L'auteur de *La contrefaçon de soi. Le cinéma à l'épreuve de la surveillance* (2021) souligne une résonance avec les courts métrages des premiers temps, notamment *A subject for the*

² Lauvin, R. (2024). *Le cinéma des formes furtives: Résister en images au regard surveillant*. Éditions Mimésis. p.10

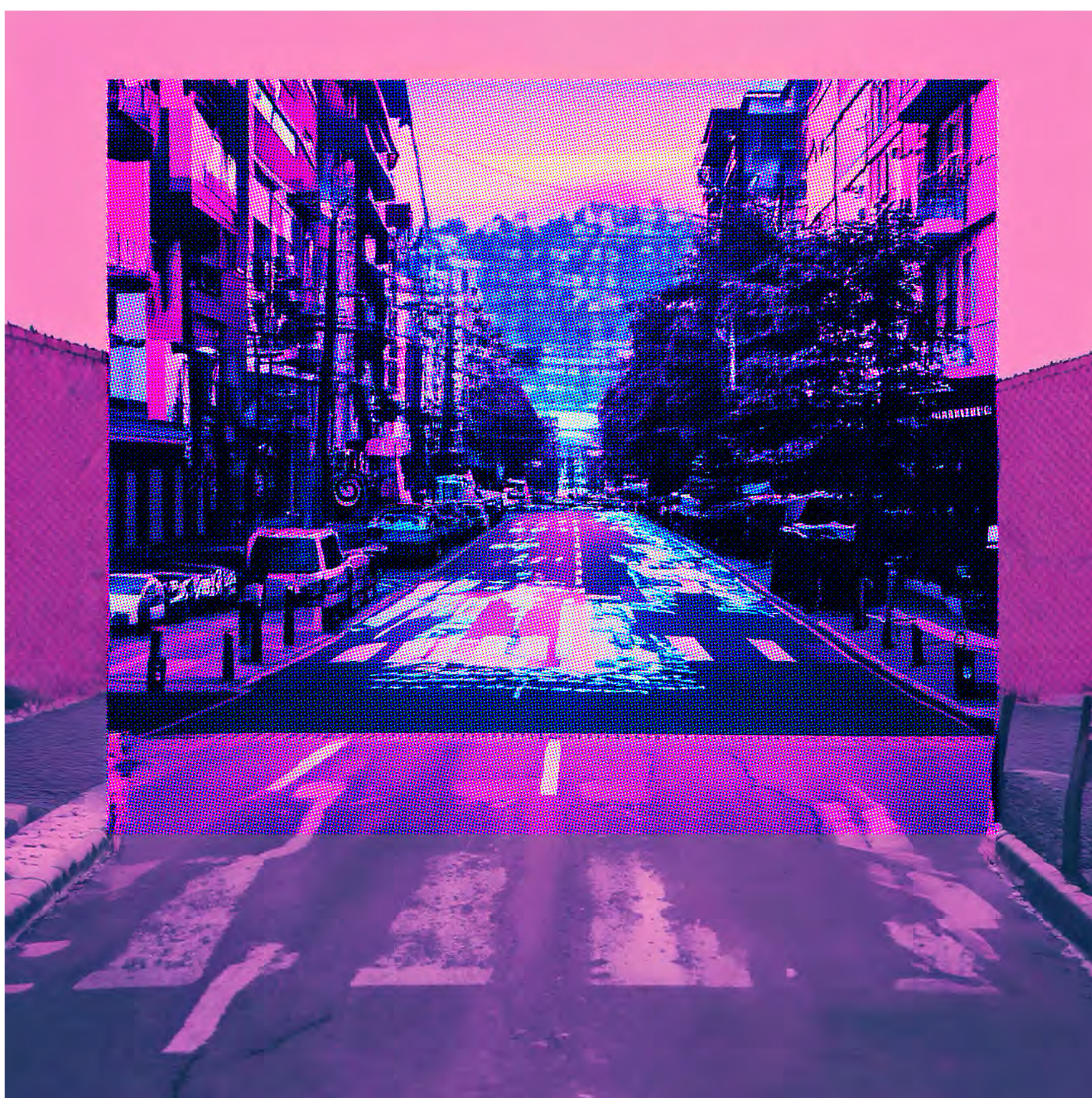


Comuzi /Surveillance View. <https://betterimagesofai.org> © BBC / <https://creativecommons.org/licenses/by/4.0/>

rogue's gallery et *Photographing a female crook* (1904), relevant selon lui de la *défiguration* (détournement de la prise de vues par une surexpressivité visuelle).

Au sein de ce front commun, **Julien Prévieux**, artiste du contre-emploi, s'attache³ à opérer un sabotage conceptuel et statistique (*statactivism*), en détournant les protocoles néolibéraux (par exemple, les lettres de non-motivation) et les brevets de gestes pour en révéler l'absurdité marchande ([What shall we do next ?](#)), tandis qu'**Éléonore Weber** et **Antoine d'Agata** s'emparent de la matérialité thermographique de la surveillance. Dans son film *Il n'y aura plus de nuit*, Éléonore Weber se réapproprie (OSINT) les images thermiques infrarouges militaires pour transformer l'œil légal du pilote en un espace de réflexion éthique, soulignant comment la vision nocturne de ces « machines de vision » aplatit le monde en une zone de cibles potentielles. Jean-Paul Fourmentraux cite à cet

³ Fourmentraux, J.-P. (2025). [Sousveillance, l'œil du contre-pouvoir](#) [Conférence en ligne, 34.10]



Elise Racine. *Is This Even Real II* / <https://betterimagesofai.org> / <https://creativecommons.org/licenses/by/4.0/>

égard les propos de **Grégoire Chamayou** : « l'éthique du combat se déplace, pour devenir une éthique de la mise à mort, une *nécroéthique*, qui utilise les principes du *jus in bello* pour les convertir en critères pertinents du meurtre acceptable »⁴.

⁴ Fourmentaux, J.-P. (2023), p.219-220

De son côté, **Antoine d'Agata** détourne ces mêmes technologies thermiques (notamment durant la pandémie, pour *Virus* ou dans ses travaux sur les modes d'existence en marge des normes sociales) pour restituer au corps sa dimension charnelle et politique, là où l'État ne cherche qu'à détecter des flux, des symptômes ou des menaces. Dans un registre différent, l'auteur de *Sousveillance* rappelle aussi le travail de l'artiste **SMITH** croisant les images thermiques avec l'ingénierie biomédicale dans l'œuvre *Cellulairement* (2012), étude pour spectres, caméra thermique et puce sous-cutanée RFID.



SuprexM10 — Travail personnel, *Smith*. CC BY-SA 4.0, [Wikimedia](#)

Ensemble, ces artistes opèrent un véritable panoptique inversé : ils n'observent pas seulement le pouvoir, ils en piratent les outils (diagrammes de Voronoï, caméras infrarouges, *tracking*, etc.) pour transformer une donnée « froide » et déshumanisée en un témoignage sensible, opérant ainsi le passage d'une surveillance subie à une sousveillance active qui réhumanise le champ de vision.

Avec la relecture bienveillante de Jean-Paul Fourmentaux



14 Dronisation de la surveillance

Dès la Première Guerre mondiale, rappelle l'entrée dédiée « drone » du *Dictionnaire du renseignement* (2020), l'expression d'« avion sans pilote » apparaît en France ; mais ledit terme « drone » est un emprunt à l'anglais désignant le faux bourdon, par altération du mot germanique *drane, dran* remontant à l'indoeuropéen °*dhron* et exprimant l'idée d'un bruit continu (*Dictionnaire historique de la langue française*, 2022). Un arrêté du 05 octobre 1984 dispose que le drone est un aérodyne sans équipage, télépilote ou programmé, utilisé pour des missions diverses. **FranceTerme** élargit cette définition suivant le *Journal officiel* du 19 juin 2011 (et la Commission spécialisée de terminologie et de néologie CSTN du ministère de la Défense) en précisant que les drones sont des engins mobiles terrestres, aériens, ou navals, sans équipage embarqué, programmés ou télécommandés, et qui peuvent être réutilisés, les drones à vocation militaire étant équipés de systèmes d'armes ou de collecte d'informations ; d'où le recours au terme de « système de drone » pour qualifier les sous-ensembles nécessaire pour faire évoluer ces appareils. Le jargon militaire français et anglo-saxon opte pour une catégorisation plus fine, sachant que l'Organisation de l'aviation civile internationale (OACI) utilise pour ces aéronefs le sigle générique RPAS (*remotely piloted aircraft system* ou système d'avion piloté à distance) :

- drones aériens appelés UAV (*unmanned aerial vehicle*, véhicule aérien sans humain à bord), UAS (*unmanned aircraft system*, système d'aéronef sans humain à bord) ou UCAV (*unmanned combat air vehicle*, drone de combat) ;
- drones de surface navals désignés comme USV (*unmanned surface vehicles*, véhicules de surface sans pilote), ASV (*autonomous surface vehicles*, véhicules de surface autonomes), USV (*uncrewed surface vessels*, navires de surface sans équipage ou plus prosaïquement navires-drones)
- drones sous-marins UUV (*unmanned underwater vehicle*, véhicules submersibles sans occupant humain), soit autonomes (AUV, *autonomous underwater vehicle*), soit téléopérés (ROV, *remotely operated underwater vehicle*) généralement par filoguidage
- drone ou robot terrestre UGV/UGS (*unmanned ground vehicle/system*, véhicule ou système terrestre sans conducteur humain à bord)

Les progrès technologiques en matière de navigation inertielle et de communication à longue distance remontent à la fin du XIX^e siècle et au début du XX^e. Ainsi, indique la revue *Les chemins de la mémoire* (n°292, automne 2025) l'ingénieur américain **Elmer Ambrose Sperry** développe en 1909 des applications pratiques gyroscopes qui permettent de stabiliser un avion en vol. Le dispositif s'appuie sur la télégraphie sans fil (TSF) dont **Gustave Ferrié**, figure importante de l'histoire de la tour Eiffel, étudie les applications militaires.

Tous ces nombreux travaux aboutissent, le 2 juillet 1917, à l'une des premières expériences de vol sans pilote, menée par le capitaine **Max Boucher** sur un avion Voisin 150 HP, à l'aide des stabilisateurs d'**Octave Détable**. À la même époque, **Archibald Montgomery Low** développe l'*Aerial Target* ; parallèlement, aux États-Unis, Elmer Ambrose Sperry, **Lawrence Sperry** et **Peter Cooper Hewitt** conçoivent le *Hewitt-Sperry Automatic Airplane*, appareil capable de lancer des torpilles aériennes. Un autre projet, baptisé *Liberty Eagle*, donne naissance au *Kettering Bug* (1918). Ce dernier constitue l'un des premiers prototypes fonctionnels de torpille aérienne sans pilote, utilisant un guidage automatique gyroscopique et un compteur de tours moteur pour s'écraser de manière autonome sur sa cible après avoir largué ses ailes. Cette architecture marque la transition historique entre l'aviation pilotée et l'ère des munitions autonomes et téléopérées.

15 Dronisation de la surveillance



© Portrait de Geoffrey Dorne
Photographie personnelle. Avec
l'aimable autorisation de l'auteur.

Geoffrey Dorne est designer et prépare un doctorat à l'Université Catholique de Lille sous la direction de Malik Bozzo-Ray au sein du Centre d'études sur les technologies de surveillance (CEThicS). Il mène une thèse à l'intersection des sciences de l'information et de la communication, des études sur la surveillance et du design graphique, explorant les stratégies de camouflage civils et militaires face aux drones sur les territoires en guerre. Son travail s'intéresse aux tactiques de dissimulation visuelle en contexte de conflit, en étudiant notamment les motifs graphiques perturbant la reconnaissance algorithmique par intelligence artificielle des drones civils à usage militaire. geoffreydorne.com



Obfuscation et contre-surveillance : les dispositifs graphiques de camouflage face aux drones sur les territoires en guerre

À une époque où les drones civils à usage militaire deviennent des outils essentiels d'observation et d'attaque, voir le cas de la guerre russo-ukrainienne avec l'usage de drones FPV du groupe tactique ukrainien Medoyid, 2022, ou encore sur les avancées du conflit au Haut-Karabagh entre l'Azerbaïdjan et l'Arménie, 2023, cette thèse⁵ cherche à étudier l'évolution des dispositifs graphiques de camouflage face à l'usage croissant des drones en contexte de guerre, afin d'identifier comment ces techniques révèlent de nouvelles formes de tactique⁶ (**De Certeau**, 1980) face à des menaces aériennes émergentes.

Les drones, avec leur capacité à capter et retransmettre des images en temps réel en survol à basse altitude, imposent une redéfinition des pratiques de camouflage par la nouvelle perspective qu'ils offrent sur le territoire (**Grevsmühl**⁷, 2014). Tant pour les forces armées que pour les populations civiles, la protection visuelle par camouflage graphique – incluant les objets, tissus, motifs mais aussi les camouflages thermiques (capes anti-IR⁸, systèmes réfléchissants), électroniques (brouillage GPS, leurres...) ou acoustiques (matériaux absorbant les signatures sonores des moteurs par exemple) – reste un enjeu stratégique. Ces tactiques doivent désormais intégrer des dimensions graphiques et technologiques pour s'adapter à ces nouvelles visées de guerre.

Aspects visuels et esthétiques du camouflage

Alors que les recherches actuelles sur le camouflage se concentrent principalement sur les aspects technologiques ou matériels (matériaux, revêtements, peintures absorbantes) – « [Asymmetric Composite Metasurface](#) », **Yanzhao W.**, 2024 – nos travaux se focalisent sur les aspects visuels et esthétiques du camouflage à l'ère des conflits « vus d'en haut », amorcés notamment par l'utilisation massive des drones par l'armée américaine en Afghanistan (opération « Haymaker », 2001 ; « Drone Papers », 2015).

Un premier temps d'analyse portera sur l'évolution des pratiques de camouflage en relation avec le corps percevant⁹ (« Phénoménologie de la perception », **Merleau-Ponty**, 1945), afin de situer ce nouveau paradigme dans une pratique préexistante. Cette recherche croisera la notion d'opérabilité des images dans la prise de décision et l'orientation stratégique, où le visuel devient un agent actif des processus opératoires (Farocki, 2000 ; Parikka, 2019) : l'image n'est plus destinée au regard humain mais devient un dispositif technique agissant directement sur le monde, « invisuelle » dans sa fonction de guidage de missiles, de

⁵ Dorne, G. [Étude des dispositifs graphiques de camouflage face aux drones sur les territoires en guerre](#).

⁶ Chez De Certeau (*L'invention du quotidien*, 1980), la tactique désigne les pratiques des dominés qui, ne disposant pas de lieu propre, doivent « faire avec » l'ordre imposé et saisir les occasions, par opposition à la stratégie du pouvoir qui planifie depuis une position de force. Ici, le terme est mobilisé dans ce sens pour qualifier les dispositifs de camouflage improvisés face à la surveillance aérienne, et non dans son acception militaire conventionnelle.

⁷ Pour une analyse de la transformation de la culture visuelle par la vue aérienne, voir l'entretien avec S. Grevsmühl : <https://sciences-critiques.fr/sebastian-vincent-grevsmuhl-il-est-urgent-de-repenser-nos-imaginaires>

⁸ Les systèmes anti-IR (anti-infrarouge) visent à réduire ou masquer la signature thermique des corps et véhicules. Les drones militaires étant équipés de caméras thermiques pour détecter les sources de chaleur, ces dispositifs (*capes réfléchissantes, tissus à faible émissivité, couvertures de survie détournées et même des voiles de forçage utilisés en agriculture...*) permettent de se soustraire à cette forme de détection en limitant ou dispersant le rayonnement infrarouge émis par le corps humain.

⁹ Chez Merleau-Ponty, le « corps percevant » désigne le corps comme condition active de la perception, situé dans l'espace et structurant notre rapport au monde. Pour le camouflage, cela implique de concevoir la dissimulation en fonction de corps observateurs situés (*pilotes, opérateurs de drones*) dont la perception dépend de leur position, mouvement et technologies de vision.

16 Dronisation de la surveillance

reconnaissance automatisée de cibles ou de navigation de drones. Cette dimension opératoire de l'image trouve une expression particulière dans la perspective verticale imposée par les drones, où la vue plongeante transforme le territoire en surface lisible et actionnable, réduisant la complexité du réel à des données analysables et exploitables militairement.



Kathryn Conrad / <https://betterimagesofai.org/> / <https://creativecommons.org/licenses/by/4.0/>

Stratégies de leurrage à l'ère des automates computationnels

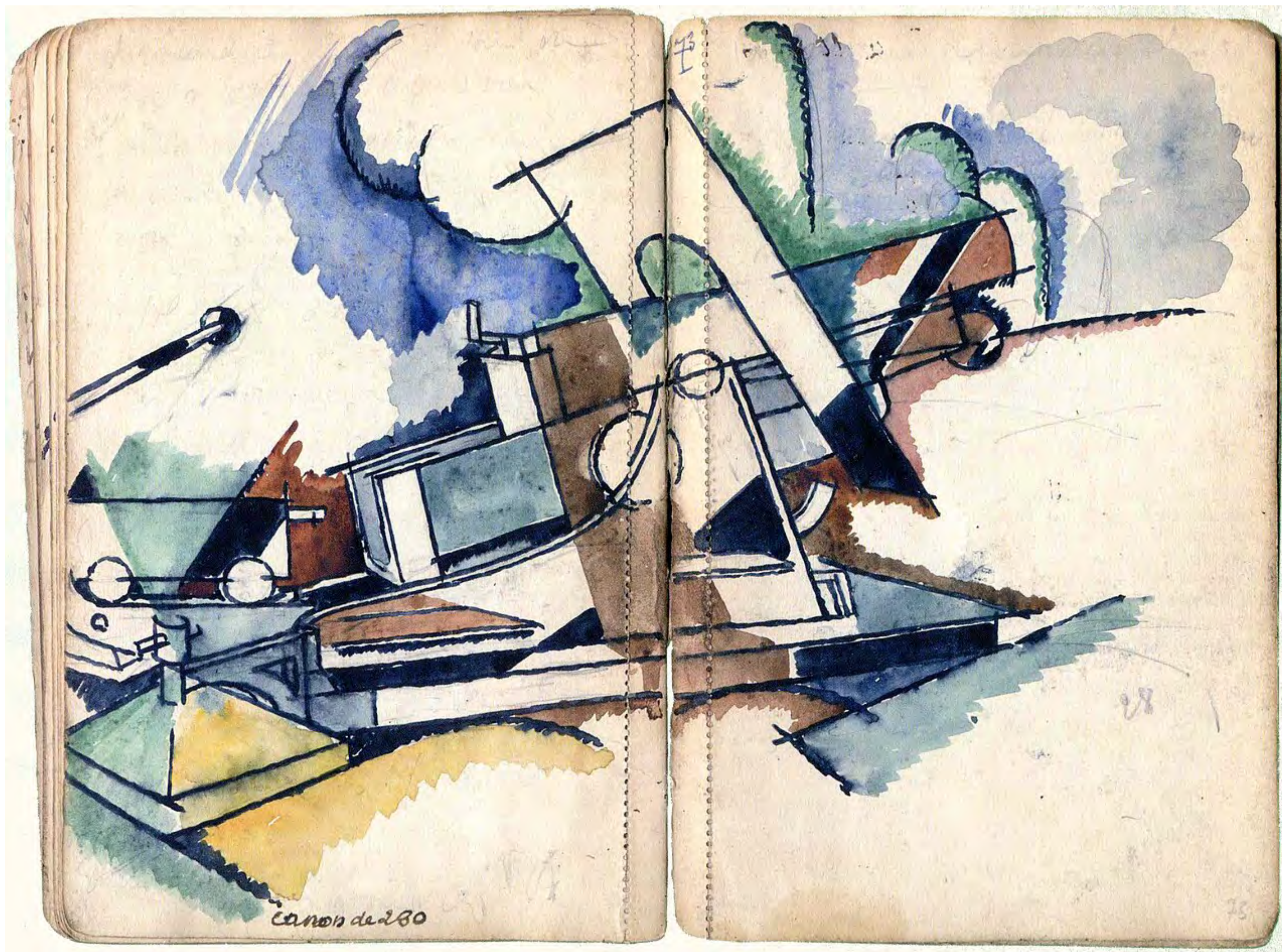
L'évolution des technologies, combinée à la diversité écologique des territoires (topographies, climats, urbanisme), exige une articulation fine entre innovations techniques et spécificités locales. L'usage des drones, dans la lignée des caméras, soulève également la problématique algorithmique de la reconnaissance de patterns, en grande partie automatisée. Les stratégies de camouflage, en mutation face aux drones, pourraient influencer des domaines plus larges comme l'urbanisme, le vêtement ou le design graphique, contribuant à une culture de la résistance visuelle. Cette recherche ambitionne ainsi de nourrir une meilleure compréhension des enjeux esthétiques liés à la protection en contexte de conflit, et d'ouvrir des pistes pour de nouvelles pratiques visuelles.

La problématique de cette thèse porte sur la nécessaire adaptation visuelle des dispositifs de camouflage graphique face aux stratégies militaires utilisant des drones civils. Avec leurs capacités de surveillance en temps réel, les dispositifs traditionnels deviennent inopérants. Comment, dès lors, des tactiques *low-tech* peuvent-elles répondre à des technologies d'observation de plus en plus sophistiquées ? Cette tension, révélatrice d'une désynchronisation technologique, pose des enjeux cruciaux pour la protection des civils et des militaires, et invite à repenser les approches graphiques et esthétiques du camouflage en zone de conflit : recouvrement de véhicules avec des matériaux du quotidien (pneus, filets de pêche, structures tubulaires), motifs disruptifs improvisés cassant les silhouettes reconnaissables, déguisements urbains transformant véhicules militaires en décharges ou en tas de ferraille, ou encore utilisation de leurres gonflables saturant les capacités de détection algorithmique.

Une disruption du regard

Un parallèle historique mérite ainsi d'être établi entre l'émergence du camouflage moderne lors de la Première Guerre mondiale et les pratiques civiles contemporaines face aux drones. L'apparition de la menace aérienne durant la Grande Guerre avait imposé une révolution des dispositifs de dissimulation, contraignant militaires et civils à inventer de nouvelles stratégies graphiques pour échapper à la vue plongeante des avions de reconnaissance.

17 Dronisation de la surveillance



Esquisse cubiste à l'encre noire et à l'aquarelle représentant un canon de campagne de calibre 280 de la Première Guerre mondiale, vers 1917, par André Mare. [Wikimedia Commons](#)

Près d'un siècle plus tard, les drones FPV reproduisent cette même disruption du regard, imposant une adaptation similaire des tactiques de camouflage (voir carte mentale ci-après). Cette récurrence interroge : assiste-t-on à un cycle historique où chaque mutation technologique de la surveillance aérienne impose une refonte complète des stratégies de dissimulation visuelle¹⁰ ?

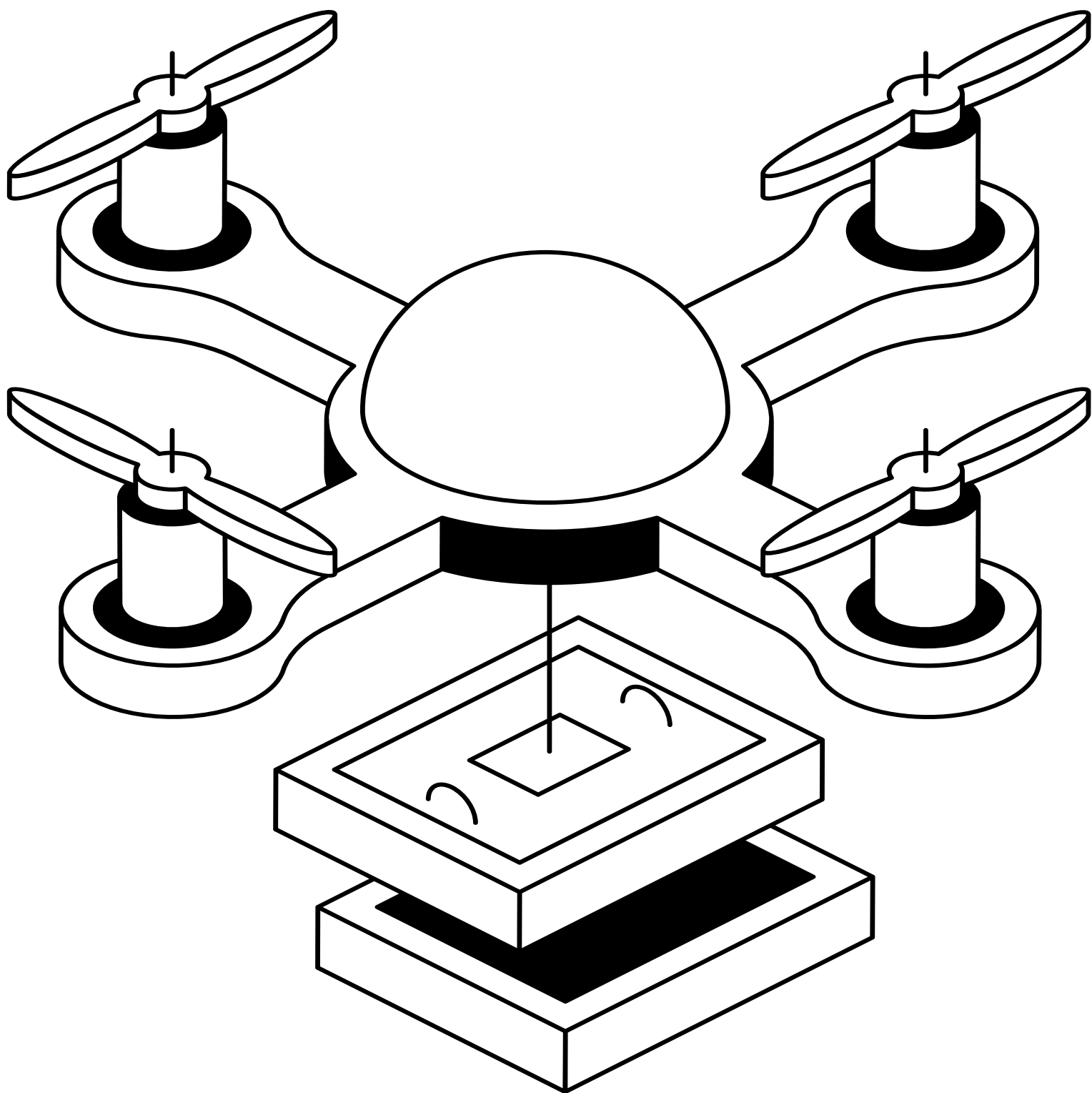
Geoffrey Dorne. Propos recueillis le 04 février 2026

« Prospectives droniques »

Le cahier central des *Chemins de la mémoire* souligne l'épineuse question des ressources en *terres rares*¹¹ (abordée dans le [cahier ÉduNum n°28 consacré à la matérialité du numérique](#)) car les drones sont « bardés de composants électroniques [ayant] un besoin vital de métaux critiques pour leurs fonctionnalités très spécialisées (caméras haute résolution, infrarouge, semi-conducteurs, moteurs électriques, etc.) ». **Océane Zubeldia**, docteure en histoire contemporaine, pour sa thèse *Mémoire et culture, genèse des systèmes de drones au service de l'homme* (2009) précise : « [...] L'autonomie des drones, en termes d'algorithmes quantiques, ne concerne pas uniquement la décision, mais permet de traiter plus rapidement d'imposants volumes de données issues de leurs capteurs, dans le cadre de transmissions ultra-sécurisées et résistantes au piratage ».

¹⁰ Le travail de l'auteur s'intéresse aux tactiques de dissimulation visuelle en contexte de conflit, en étudiant notamment les motifs graphiques perturbant la reconnaissance algorithmique par intelligence artificielle des drones civils à usage militaire. À travers une approche combinant analyse des dispositifs technologiques, OSINT, ethnographie par le design et étude des stratégies de camouflage en zones de guerre, il cherche à comprendre comment le design graphique peut devenir un outil de contre-surveillance et de transformation du pouvoir. Il intervient également dans le domaine du design critique et technopolitique, questionnant les impacts visuels des technologies de surveillance sur nos environnements contemporains

¹¹ Rappelons que cette expression, trompeuse, de l'ordre de l'artefact marketing suggère une rareté qui n'existe pas géologiquement, mais qui découle de la complexité de leur concentration économique. Les ETR, éléments de terres rares, ne sont pas rares et sont en général plus abondants que les métaux précieux comme l'or ; ce ne sont pas non plus des terres (voir [rapport de l'ESCO](#)).

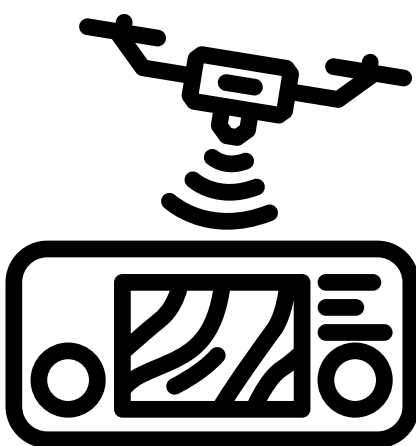


Typologie des drones en contexte militaire

Fonction			Altitude		Détection		
Reconnaissance	Attaque	Logistique	Haute	Basse	Optique	IR	Multi-spectral
MQ-9 Reaper	FPV Kamikaze	Cargo	Global Hawk	DJI Mavic	Caméra HD	Thermal FLIR	Combiné radar+IR
Bayraktar TB2	Lancet	Matrice	RQ-4	FPV Racing			
Orlan-10	Shahed-136			Quadricoptère artisanal			



Implications pour le camouflage

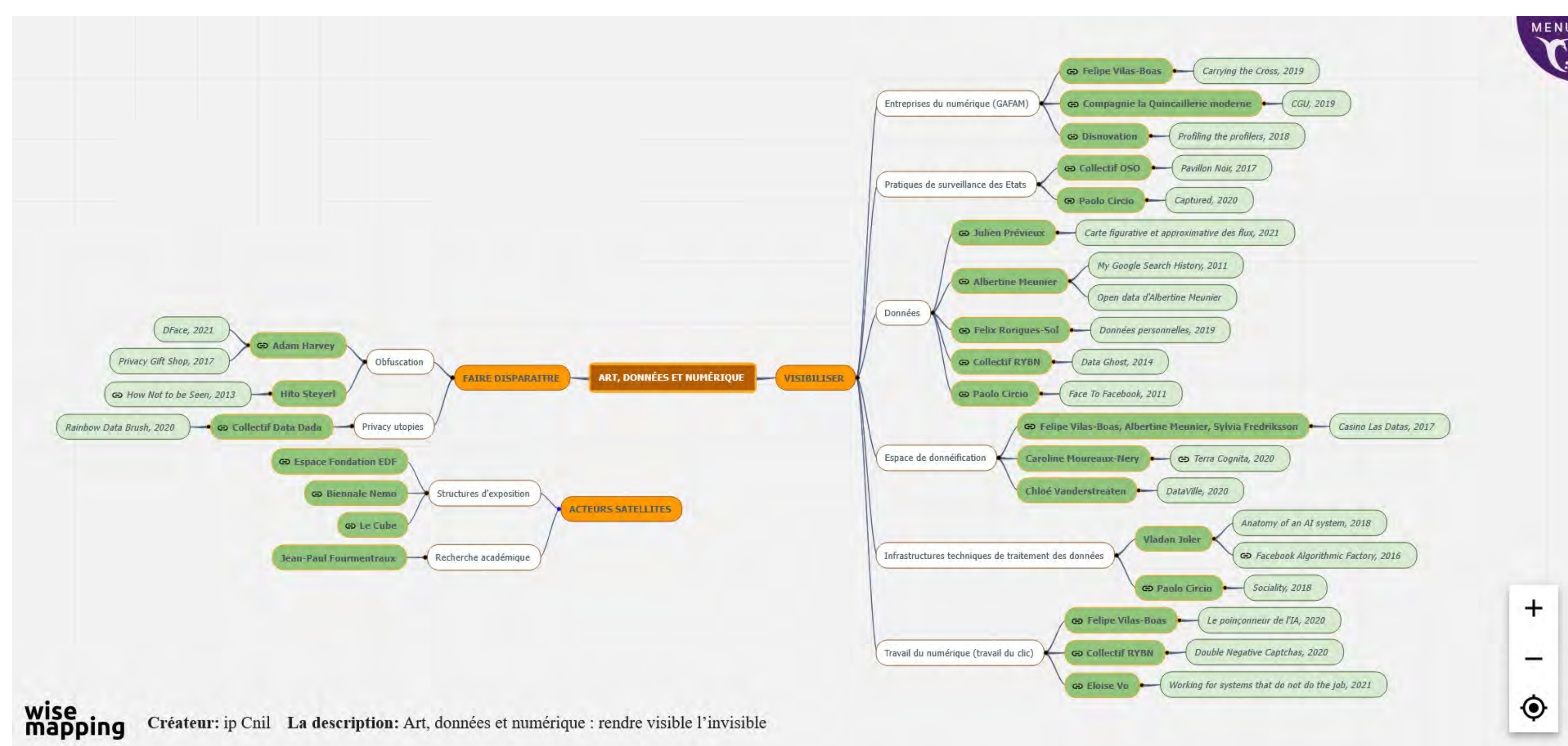


Vue plongeante perpendiculaire	Temps réel (retour vidéo)	Automatisation (reconnaissance IA)
Motifs disruptifs horizontaux requis	Adaptation rapide des tactiques, brouillage	Saturation des algorithmes par leurres/patterns

Le regard surveillancier

Nous vivons une époque marquée par une omniprésence des dispositifs de surveillance prenant des formes variées comme des caméras urbaines, des drones, des objets connectés ou des systèmes de collecte massive de données. Cette surveillance, désormais banalisée et institutionnalisée, tend à s'imposer comme un instrument central de contrôle et de régulation sociale, redéfinissant potentiellement les rapports de pouvoir et les limites de la vie privée. Dans ce contexte, la notion de regard en art s'avère particulièrement éclairante. Elle nous pose des questions portant sur des mécanismes de la visibilité, interrogeant de fait comment le pouvoir s'exerce par la capacité de voir, de rendre visible et de dominer par la vision, par la puissance qu'elle apporte à qui la possède et la domine. En ce sens, le « regard panoptique », tel que théorisé par **Michel Foucault** dans [Surveiller et Punir](#) (1975), fonctionne comme un mécanisme invisible mais omniprésent, assurant l'efficacité du pouvoir par sa seule potentialité, même lorsqu'il n'est pas explicitement exercé. Pourtant, malgré son apparente immatérialité, ce regard devenu numérique conserve une réalité concrète, dont les effets se manifestent dans les comportements, les normes et les contraintes qu'il impose.

C'est précisément dans ce cadre que le champ artistique émerge comme un terrain d'observation et de résistance privilégié. N'y étant plus subie passivement, la surveillance y est dénoncée, détournée ou subvertie. En cela, l'art ne se limite pas à une simple expression esthétique. Il incarne aussi une force éthique, parfois politique, capable de révéler les mécanismes de la surveillance et d'inventer des stratégies de résistance. Les artistes, par des démarches telles que l'obfuscation, le camouflage, la désobéissance ou le contournement des systèmes, exploitent les failles de ce pouvoir de la surveillance. En la transformant en objet de réflexion et d'action, ils ouvrent des brèches dans l'économie du visible, invitant le spectateur à interroger son rapport à un monde où le regard est à la fois ubiquitaire et contesté. La Lettre ÉduNum n°19 *Cybersécurité* aborde cette stratégie de [l'obfuscation artistique](#) comme mode de résistance face à un pouvoir contrôlant le regard et ses impacts sur nos comportements (cartographie des acteurs et pratiques ci-dessous).



Art et données : une cartographie contributive, rendre visible l'invisible, 2022. *LINC* [en ligne]. [Consulté le 8 mai 2026].
Disponible à l'adresse : <https://linc.cnil.fr/art-et-donnees-une-cartographie-contributive>. CC-BY 4.0 FR

Cette contribution explore les liens complexes entre art, pouvoir et surveillance, en analysant la manière dont les artistes décryptent, citent, détournent ou critiquent les mécanismes de la société surveillée, tout en révélant comment leurs œuvres peuvent

refléter les tensions et dérives de la surveillance généralisée. Selon **Andrea Brighenti**, dans [Artsurveillance : at the crossroads of art and surveillance](#) (2010, CC BY-NC-ND), deux postures artistiques distinctes émergent face à ce phénomène. D'une part, les artistes qui intègrent la surveillance au cœur de leur processus créatif, et d'autre part, ceux qui s'approprient les technologies de surveillance elles-mêmes pour en faire un médium artistique. Ces deux démarches, bien que différentes, interrogent ce regard surveillant qui s'immisce dans notre quotidien par l'intermédiaire des caméras et dispositifs de contrôle.

Face à l'omniprésence de ces infrastructures, Brighenti identifie trois stratégies artistiques marquantes. Certains artistes représentent ou matérialisent ce regard intrusif, le rendant tangible pour le spectateur ; d'autres l'incarnent, en développant une esthétique évoquant les systèmes surveillancielles ; enfin, une troisième approche consiste à fabriquer des équipements de surveillance fictifs détournant, déformant ces mécanismes à l'œuvre.



Jamillah Knowles & Digit / <https://betterimagesofai.org> / <https://creativecommons.org/licenses/by/4.0/>

Les multiples recherches artistiques dénonçant ces systèmes d'oppression ne se limitent pas à une simple mise en scène esthétique. Elles cristallisent et dénoncent des systèmes autoritaires qui souhaitent contrôler le visible. Entre symbolique, esthétique et politique, ces dispositifs de surveillance façonnent notre perception du monde en fabriquant par la maîtrise du visible de nouveaux récits. Il ressort ainsi que le champ du visible n'est pas neutre. En effet, il est toujours médiatisé par des codes, des langages et des rapports de force, introduisant une asymétrie fondamentale entre celui qui observe et celui qui est observé. Cette dissymétrie visuelle transforme alors l'espace perceptif en un terrain stratégique, où tout ce qui est vu devient, potentiellement, un objet de contrôle. Il s'agit d'une dynamique que les artistes exploitent pour révéler, contester ou subvertir les logiques de la surveillance.

La [ressource pédagogique de l'académie de Toulouse](#) en arts plastiques interroge *Les dangers de la surveillance sur le net* en s'appuyant sur la conférence de **Julien Vaubourg** *Je n'ai rien à cacher*, captée en 2015 à l'université de Lorraine, dans une logique de sensibilisation des enseignants, chercheurs et étudiants à la protection des données privées dans le cadre de leur enseignement.



**ACADÉMIE
DE TOULOUSE**

*Liberté
Égalité
Fraternité*

L'artiste, géographe et chercheur **Trevor Paglen** oriente sa pratique artistique vers une exploration méthodique des zones opaques du pouvoir, qu'il s'agisse des mécanismes étatiques, militaires ou économiques dissimulés aux regards ayant pour objectifs de façonner notre perception du réel faisant émerger ainsi de nouveaux récits. Paglen privilégie une analyse systémique des structures invisibles qui régissent nos sociétés, en s'attachant à décrypter leurs logiques, leurs enjeux et leurs conséquences. La mention de cette œuvre de Trevor Paglen se retrouve dans la [Lettre ÉduNum thématique *Esthétiques de l'artificiel*](#) publiée en 2024. Cette dernière invite à découvrir son travail artistique, nourri par une rigueur scientifique, reposant sur une collecte minutieuse et massive de données, leur recoupement et leur vérification, afin de mettre au jour des réalités occultées.



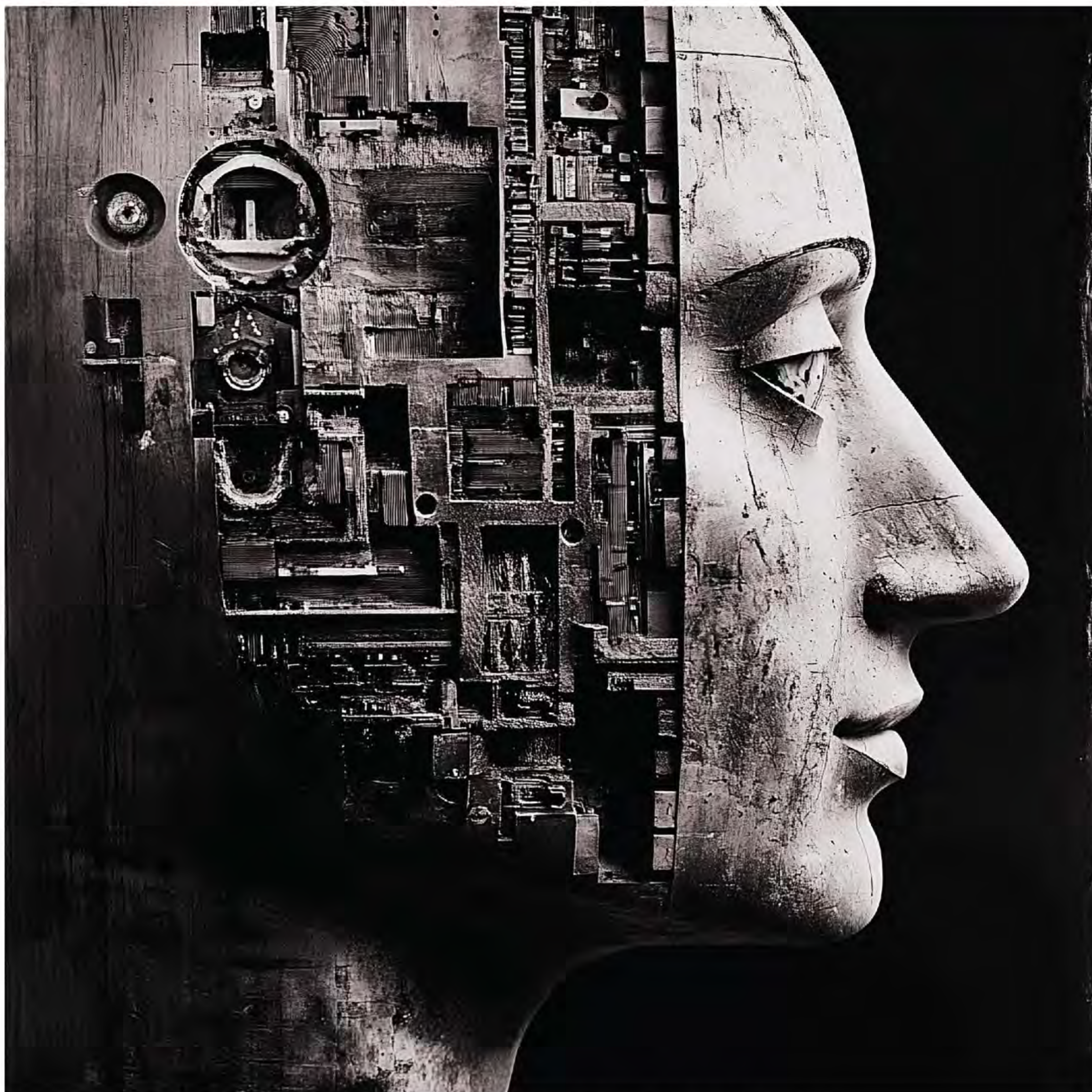
MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

*Liberté
Égalité
Fraternité*

Lettre d'information sur le numérique éducatif



**Esthétiques
de l'artificiel**
N°24
Octobre 2024
(mise à jour mai 2025)



Artwork ©Thierry Murat with Midjourney --v 5.2. Expérience d'intelligence
artistique (IA) : poétique du *prompt*. Avec l'aimable autorisation de l'auteur.

L'artiste adopte des méthodes intrusives déconstruisant les mécanismes à l'œuvre dans les systèmes surveillanciers pour en révéler les impacts sur le corps social et la transformation de notre regard. Il tente ainsi de saisir le réel dans ses replis les plus insaisissables en mobilisant des technologies sophistiquées pour capter ce qui échappe délibérément à toute visibilité humaine. Que ce soit par une immersion directe ou une médiation technologique, sa démarche artistique témoigne de son engagement à rendre visible l'invisible, transformant l'art en un levier de connaissance et de critique sociale.

L'inversion du regard surveillancier

Dans le champ de l'art contemporain, certains artistes interrogent la notion de surveillance en transposant le regard surveillancier en un œil métaphorique, à l'image de la [série *Today is great*](#) (2014) de **Julien Prévieux**. L'artiste utilise un téléobjectif pour scruter les bureaux de Google, situés au deuxième étage du Binoculars Building, édifice emblématique conçu par **Frank Gehry** à Los Angeles. Les clichés révèlent la vie quotidienne des employés par l'intermédiaire de notes manuscrites ou de croquis humoristiques, autant de fragments d'une activité professionnelle qui doit être dissimulée au regard de tous. Julien Prévieux transforme ces photographies en une série de dessins à l'encre de Chine, fixant ces instants volés en leur conférant une esthétique poétique à dimension artistique. Par ce geste, il inverse délibérément les rapports de pouvoir contre les géants du numérique qui captent et exploitent nos données personnelles. L'artiste propose une riposte symbolique, en retournant le regard surveillancier contre ses propres auteurs. Il crée une faille ironique dans le dispositif de sécurité des systèmes de contrôle pour épier ceux qui nous épient. Julien Prévieux, par ce biais, s'engage dans une forme d'art de résistance en détournant les logiques de contrôle et en jouant avec les codes de la visibilité et de l'invisibilité.



Leo Lau & Digit / <https://betterimagesofai.org> / <https://creativecommons.org/licenses/by/4.0/>

La réappropriation des mécanismes de visibilité et résistance se trouve au cœur du processus créatif de **Mohamed Bourouissa**. Dans sa pratique artistique, l'artiste défie les mécanismes de l'invisibilisation imposée par la prison sur les prisonniers eux-mêmes. Pour Bourouissa, il s'agit de rendre une présence à ceux que le système pénitentiaire condamne à n'être que des sujets/objets de surveillance. En brisant cette asymétrie, l'artiste questionne la nature des secrets imposés par les systèmes de surveillance tout en interrogeant les discours qui produisent ces secrets.

Son film [Temps mort](#) réalisé en 2009, titre emprunté au rappeur Booba, illustre cette démarche artistique de résistance dans une approche subversive confinant à l'illégalité. Ainsi, produit dans la clandestinité, ce projet contourne les interdits en s'appuyant sur un échange de SMS, MMS et séquences filmées entre l'artiste et deux détenus. Les images, capturées à l'aide de téléphones portables échangés entre l'artiste et les prisonniers deviennent ainsi le témoignage brut d'une réalité carcérale tout en incarnant un acte de défiance vis-à-vis de cette même institution. L'esthétique de ce film composite en basse résolution laisse transparaître une forme d'intimité. Certains artistes se saisissent de ce questionnement en proposant des expériences immersives reproduisant et incarnant le point de vue même du regard surveillancier. Une forme de renversement s'opère, plongeant

ainsi le spectateur dans la position du scrutateur. L'installation interactive *Jaywalking* (2015) de **Dries Depoorter** en est une illustration frappante. Elle permet aux spectateurs de se connecter en direct à des flux vidéo de caméras de surveillance urbaines, disséminées à travers différents pays, et de jouer le rôle d'un agent de contrôle, en offrant la possibilité de repérer les piétons traversant en dehors des « passages cloutés ». Plus troublant encore, l'œuvre délègue au public le pouvoir de sanction. Un simple appui sur un bouton suffit pour envoyer une capture d'écran de l'infraction aux autorités locales, transformant ainsi le spectateur en complice actif du système surveillanciel. Ce renversement des rôles dénonce avec ironie l'impact de ces dispositifs sur notre capacité d'agir marquant comme une forme d'assujettissement de l'humain par les mécanismes de surveillance et d'oppression.



Comuzi / <https://betterimagesofai.org/> / © BBC / <https://creativecommons.org/licenses/by/4.0/>

À l'instar de l'artiste **Banksy** et de son dispositif de vidéosurveillance positionné contre un mur sur lequel est inscrit *What are you looking at ?* les artistes contemporains qui tentent de dénoncer l'omniprésence de ces systèmes de surveillance dans notre société contemporaine les détournent dans une visée à la fois ironique et cynique. Ainsi, ces

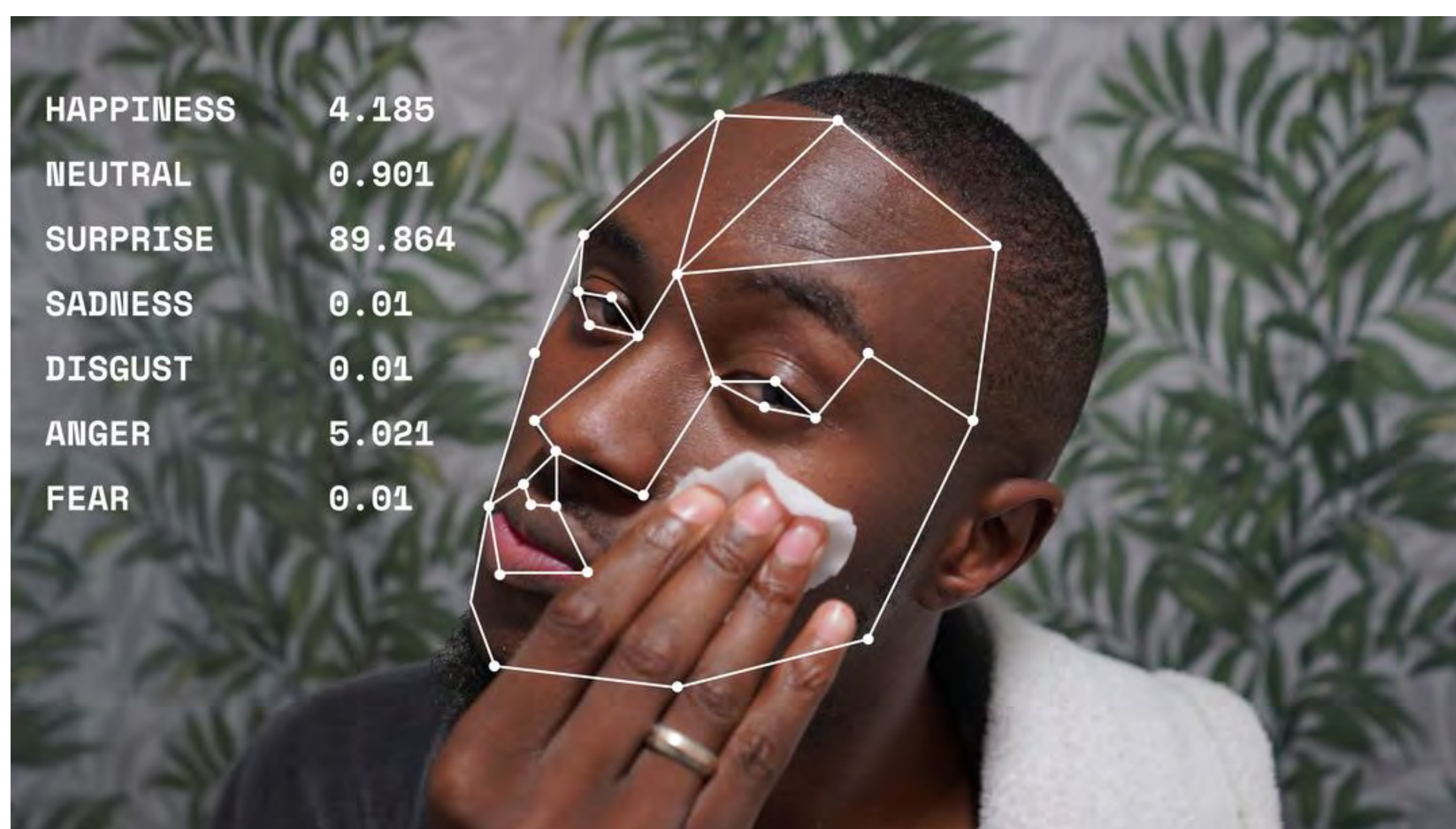


Pauline Wee & DAIR / <https://betterimagesofai.org/> / <https://creativecommons.org/licenses/by/4.0/>

démarches artistiques contemporaines ne se contentent pas de dénoncer les mécanismes de la surveillance, ils les subvertissent en déployant des dispositifs de détournement et d'altération des systèmes de contrôle visuel, comme pour en révéler les failles et les excès. Au cœur de ces expérimentations, les artistes questionnent l'omniprésence et la portée de la vision artificielle dans une logique d'opposition à la perception humaine. Cette vision déshumanisée, où la caméra, couplée à des algorithmes, ne se contente plus de capturer des images, mais les analyse, les interprète et en extrait un sens de manière autonome sans médiation humaine, nous questionne sur ce pouvoir machinique et cette mise à l'écart de toute vision humaine.

Dispositifs surveillanciers, entre surveillance et contrôle de nos sens

La transformation numérique de la surveillance bouleverse profondément notre rapport au monde, modifiant non seulement nos représentations de la réalité, mais aussi nos manières de l'habiter, de nous y déplacer et d'y interagir. Une part croissante de notre perception est désormais déléguée à des machines, qui ne se contentent plus de capturer des images mais les analysent et les interprètent. L'un des exemples les plus frappants réside dans le traitement algorithmique des expressions faciales. Ces technologies ne se limitent plus à enregistrer un visage, elles l'identifient, elles décryptent ses émotions, voire anticipent ses intentions.



Comuzi / <https://betterimagesofai.org> / © BBC / <https://creativecommons.org/licenses/by/4.0/>

Trevor Paglen questionne ce champ de la reconnaissance faciale par les intelligences artificielles analytiques dans son œuvre [*Behold These Glorious Times !*](#) (2017). L'artiste propose une expérience visuelle immersive et fragmentée, où deux catégories d'images s'entrelacent. D'un côté, il puise dans d'immenses bases de données, des corpus d'images standardisées utilisées pour entraîner les algorithmes de reconnaissance visuelle à identifier des objets, des visages, des gestes ou même des émotions. De l'autre, il révèle au spectateur ce que perçoivent réellement ces systèmes. À travers ce montage composite, Trevor Paglen plonge le spectateur au cœur des enjeux épistémologiques et politiques de la vision artificielle, interrogeant les biais, les limites et les dangers de ces technologies qui, loin d'être neutres, façonnent notre rapport au réel ainsi que notre culture visuelle contemporaine.

L'artiste nous montre que les dispositifs surveillanciers illustrent cette volonté de décoder le visible afin de le reconfigurer à travers des dispositifs de vision augmentée par l'IA. Le visage humain, autrefois domaine de l'intimité et de l'interprétation subjective, est aujourd'hui soumis à des systèmes de détection, de reconnaissance s'appuyant sur les nouveaux modèles d'intelligence artificielle qui tentent d'orienter nos actions et nos choix. Ces machines de vision augmentée de plus en plus autonomes simulant l'intelligence humaine grâce à des mécanismes d'apprentissage automatique (*machine learning*), opèrent selon des logiques opaques. Leur fonctionnement, bien que sophistiqué, échappe en partie à notre compréhension, tout en exerçant une influence grandissante sur nos vies. À l'ère de la détection généralisée, nous sommes devenus à la fois les cibles et les objets de ces dispositifs, qui observent nos réactions, captent nos émotions en tentant d'orienter nos décisions. Dans un contexte marqué par l'anxiété et l'hyperstimulation sensorielle, le pouvoir ne s'exerce plus seulement par la contrainte, mais à travers une emprise sur nos sens. La capacité à orienter, médiatiser et monétiser le sensible constitue désormais l'un des fondements de la domination contemporaine, où la gestion des affects devient un outil de gouvernance. Dans son œuvre [*Faces of ImageNet*](#) (2022) Trevor Paglen, grâce à une

caméra de surveillance camouflée, film les spectateurs entrant de façon inconsciente dans le cadre de l'image. Une fois saisi par le système, le visage devient le point de départ d'un processus automatisé de reconnaissance faciale et d'étiquetage par des mots-clés rattachés à des ensembles d'images préexistantes provenant de la base de données controversée ImageNet. Par ce dispositif, l'artiste accentue les biais et les stéréotypes générés par les intelligences artificielles génératives afin de dénoncer la volonté de classification du réel et de nos émotions par ces dernières à des fins de contrôle.

Un certain nombre d'artistes contemporains se saisissent des logiques appliquées aux mécanismes de surveillance en tentant de les détourner par la dérégularisation ou la neutralisation de leurs fonctions premières. L'œuvre [Face to Facebook](#) (2011), de l'artiste **Paolo Cirio** met en lumière les mécanismes à l'œuvre développer par les réseaux sociaux pour contrôler nos sens. Pour ce faire, il a extrait les données personnelles d'un million de profils Facebook, avant de les réinvestir dans un faux site de rencontres, où les affinités entre utilisateurs étaient générées par un algorithme de reconnaissance faciale analysant leurs expressions. Ce détournement opéré par l'artiste dénonce les failles et les biais des systèmes de collecte massive et leur impact sur nos vies affectives en dehors de toute dimension éthique.

Au-delà des enjeux liés à la surveillance généralisée se pose la question de notre dépendance aux technologies numériques et de la manière dont nos gestes quotidiens nourrissent l'extraction massive de nos données personnelles. C'est cette relation ambiguë, presque symbiotique, que nous entretenons avec nos outils connectés qu'explore l'artiste et activiste russe **Dasha Ilina** en posant sur ces interrelations un regard à la fois caustique et désenchanté. Le projet [Center for Technological Pain](#) (CTP) développé avec des solutions *low-tech* propose de panser les maux réels ou imaginaires engendrés par une exposition excessive aux écrans.



Julieta Longo & Digit / <https://betterimagesofai.org/> / <https://creativecommons.org/licenses/by/4.0/>

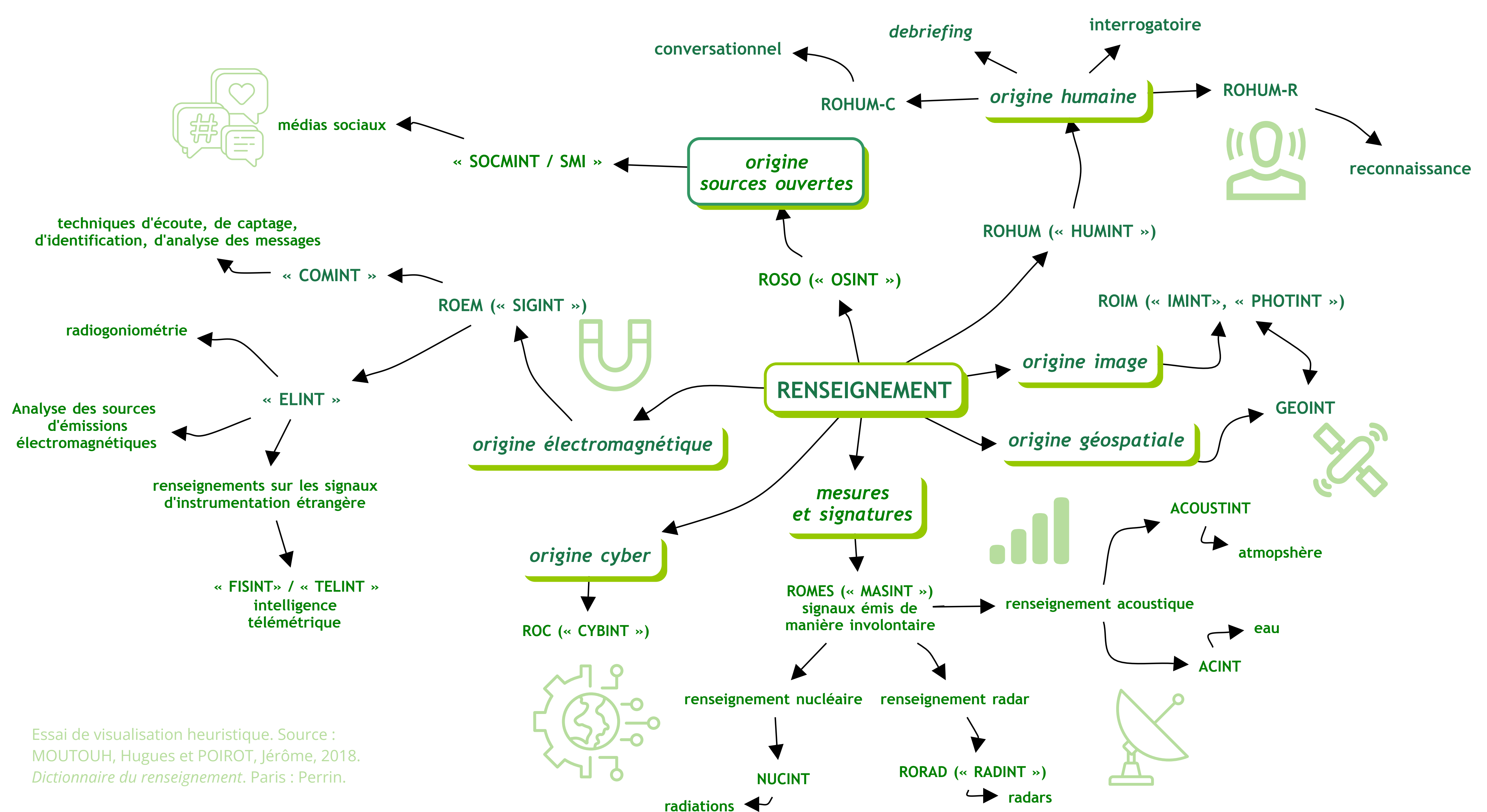
Cette approche interroge potentiellement tout un chacun sur les liens tissés avec ces nouvelles technologies qui parviennent à pénétrer de plus en plus le champ de l'intériorité. En cela, elle dénonce les pratiques de collecte biométrique, désormais omniprésentes, servant d'outil pour créer des documents d'identification à destination des différents services administratifs et permettant d'étendre, jour après jour, leur emprise sur des aspects toujours plus intimes de notre identité.

Sources ouvertes, enquêtes, surveillances et ingérences

L'appréhension des conflictualités informationnelles contemporaines requiert l'élaboration d'une taxonomie cohérente des diverses notions associées à ces désordres épistémiques : mésinformation, désinformation, malinformation (► [Vidéo ODIL](#)), influence, ingérence, etc.) ainsi qu'une cartographie précise des méthodes plurielles d'investigation numérique et de vérification des faits, à l'ère de la [post-vérité](#) ou de la post-factualité (Deneuve, 2025). En effet, le flou terminologique constitue un obstacle certain à la compréhension approfondie des enjeux et mécanismes liés aux [manipulations de l'information](#).

De la donnée brute à l'OSINT

Une démarche structurée de vérification de l'information exploite les sources ouvertes, notamment l'OSI(N)F ou *open source information*. Ce large spectre englobe tout un ensemble de données publiques accessibles (OSD, *open source data*) qu'il s'agisse de rapports gouvernementaux, de documents administratifs, de contenus générés par les utilisateurs (CGU) comme les publications sur les réseaux sociaux, d'articles de presse ou d'archives du web consultables depuis la *Wayback Machine* d'Internet Archive, les vues satellitaires et données géographiques, le suivi en temps réel des vols d'aéronefs ou du trafic maritime, etc. Cette matière première, disparate et non filtrée, correspond aux traces que tout individu ou organisation dépose naturellement en ligne, volontairement ou involontairement, issues de ses pérégrinations et interactions dans le cyberspace ou des empreintes héritées et liens connexes que d'autres tissent autour de ces mêmes identités. L'OSINT, ou en français, renseignement d'origine sources ouvertes (ROSO), désigne quant à lui la méthodologie permettant de transformer ces données éparsément accessibles sur les réseaux en du renseignement utile pour *investiguer* et analyser une situation particulière traitant d'enjeux de guerre, de sécurité nationale, d'intelligence économique, ou encore de déstabilisation informationnelle (Mercier, 2025). À travers ce prisme hyperdocumentaire (Le Deuff, 2021) se positionnent désormais de nombreux acteurs, dont le journalisme d'investigation (parfois repris dans l'acronyme



OSINV (► [scénario](#) de l'**académie de Reims** ) , au cœur d'un écosystème plus vaste de méthodes d'analyse dites « **INT**elligentes » : ces approches se spécialisent et se distinguent et précisent par la variation de leur préfixe (GEONINT, HUMINT, MASINT, SIGINT, TELINT, etc.), chaque combinaison pointant vers une source d'information et une technique d'analyse spécifique. À l'opposé de l'OSINT se trouve le CSINT (*closed source intelligence*), correspondant au renseignement issu de sources fermées, privées ou protégées. Contrairement à l'OSINT qui agrège des données puisées dans le « domaine public », le CSINT opère dans des environnements non accessibles à tous, tels que les bases de données sécurisées, les communications chiffrées internes, ou les réseaux privés.

Cependant, la frontière entre le CSINT et l'OSINT devient particulièrement poreuse lorsque l'on intègre le rôle des [lanceurs d'alerte](#) qui transforment des données confidentielles, sensibles ou classifiées en informations exploitables à grande échelle. Un ensemble de cas emblématiques, comme Wikileaks (fondée par **Julian Assange** en 2006), les révélations d'**Edward Snowden** en 2013 ou les fuites des Panama Papers en 2016 (en référence aux Pentagon Papers de la guerre du Vietnam), illustrent bien comment le CSINT bascule dans le champ de l'enquête publique. D'autres termes gravitent autour de l'acronyme OSINT comme la *forensique* désignant des pratiques scientifiques associées aux investigations judiciaires (médecine légale, linguistique forensique, informatique forensique) ou celui de *contre-enquête* à dimension militante et parfois sujette à des dérives complotistes ou conspirationnistes (Deneuville, 2025).

La dimension pharmacologique de l'OSINT

En s'appuyant sur une conceptualisation philosophique héritée de la pensée derridienne (développée par **Jacques Derrida** dans son exégèse du *Phèdre* de **Platon** et notamment reprise par **Bernard Stiegler**), le chercheur **Allan Deneuville** définit l'OSINT comme un *pharmakon*, agissant simultanément comme remède et poison. Dans sa fonction curative, l'OSINT opère comme un instrument de transparence et de contre-pouvoir au sein de la sphère démocratique. Il confère aux chercheurs, aux professionnels de l'information et aux citoyens-enquêteurs lambdas la capacité épistémique de documenter les violations des droits humains, de vérifier et contrecarrer la parole publique, permettant de résorber les asymétries informationnelles structurelles. Ce faisant, l'OSINT constitue un instrument de vigilance citoyenne. Toutefois, cette méthodologie comporte une face obscure et toxique qu'Allan Deneuville qualifie de « dark OSINT », exposant des dérives potentiellement antidémocratiques et délétères comme la traque obsessionnelle et prédatrice (*stalking*) ou la divulgation malveillante d'informations personnelles (*doxxing*). La faculté d'agrégation de données publiques, initialement conçue pour l'enquête, qu'elle soit interpersonnelle ou systémique, se métamorphose alors en dispositif de surveillance, voire en « vigilantisme ». ([Dulaurans](#), 2024). Ces instrumentalisation peuvent donner lieu à des campagnes de harcèlement numérique ou préfigurer d'autres formes d'exactions par l'exploitation des vulnérabilités informationnelles des cibles visées. Ainsi, l'OSINT incarne cette dialectique pharmacologique, oscillant entre la consolidation de la transparence citoyenne et la subversion des libertés démocratiques fondamentales.

Ingérences et manipulations informationnelles

L'ingérence (► [Vidéo Lumni](#)) en droit international désigne le fait pour un État ou une organisation internationale d'intervenir dans les affaires intérieures d'un pays tiers, sans son consentement. Cet acte est perçu comme illégitime car contraire au principe de souveraineté (article 2, alinéa 7, [Charte des Nations Unies](#)). En matière informationnelle « les ingérences consistent à diffuser de fausses informations pour influencer les jugements



Francesco Hayez. *Les derniers instants du doge Marino Faliero*. Huile sur toile, pinacothèque de Brera. [Wikimedia Commons](#)

de l'opinion publique et les décisions politiques, à semer la confusion informationnelle pour paralyser le jugement, à discréditer et harceler en ligne des adversaires politiques et à interférer dans les élections » (Mercier, 2025). Face à ces menaces, l'appareil d'État français a dû adapter son architecture sécuritaire. VIGINUM (créé en 2021), service de l'État chargé de la protection contre les ingérences numériques, illustre la mise en pratique de l'OSINT défensif. Les opérations de manipulation de l'information et d'ingérence¹¹ depuis l'étranger détectées sur le territoire national démontrent une ingénierie complexe. L'analyse par exemple de la campagne de désinformation pro-russe baptisée Matriochka (► [Décryptage](#) par **Hervé Letoqueux** ) révèle un mode opératoire spécifique ciblant les mécanismes de vérification, notamment les comptes sociaux des médias et des vérificateurs de faits occidentaux pour les inonder de narratifs anti-ukrainiens. L'action de l'État s'est aussi matérialisée en juillet 2024 par la signature d'une [convention cadre de partenariat entre l'Autorité de régulation de la communication audiovisuelle et numérique \(Arcom\) et VIGINUM](#). Au cours du même mois a été promulguée la [Loi du 25 juillet 2024 visant à prévenir les ingérences étrangères en France](#). L'urgence de cette mobilisation est corroborée par les travaux de l'Assemblée nationale, qui a rendu en décembre 2025 un rapport d'information édifiant sur l'irruption de l'intelligence artificielle dans les ingérences étrangères. L'analyse de la campagne russe Storm-1516, documentée comme l'opération de désinformation la plus étendue jamais enregistrée sur le territoire national avec plus de 55 millions de vues générées et 38 877 publications sur les réseaux sociaux, démontre comment l'automatisation computationnelle permet de saturer l'espace public avec des coûts de production marginaux. Le rapport souligne en outre que les attaques par empoisonnement des données font de l'intelligence artificielle à la fois un outil et une cible d'ingérence. Les rapporteurs émettent enfin dix-huit propositions stratégiques pour bâtir un bouclier démocratique, préconisant, entres autres, l'instauration d'un consentement obligatoire aux algorithmes de recommandation, la création d'une réserve algorithmique en période pré-électorale pour éviter toute manipulation, le renforcement substantiel des moyens humains et techniques de VIGINUM ainsi que la nécessité d'une labellisation informationnelle associée à un score d'artificialité indiquant dans quelles proportions l'IA a été utilisée pour générer les contenus.

¹¹ Voir le concept de [FIMI](#)



Pour la première fois, l'homme abandonne sa prérogative cognitive à un élément exogène. Ce basculement a ainsi pu justifier, selon certains, que soit acté le passage à une nouvelle époque, « l'âge de l'intelligence artificielle ». Après l'âge de la religion, marqué par un monopole ecclésiastique de l'information, puis l'âge de la raison durant lequel l'humanité a pris conscience de sa capacité à penser le monde par le doute et la recherche de vérité, serait venu le temps d'une intelligence annexe remettant en cause la matrice cartésienne *cogito ergo sum*, « je pense donc je suis ».

– *Rapport d'information sur l'irruption de l'intelligence artificielle dans les ingérences étrangères* (2025)

Comment parler des manipulations de l'information en classe ?

Au-delà de la réponse technologique et institutionnelle, la nécessaire résilience cognitive passe par une transposition de ces enjeux complexes à des formats pédagogiques adaptés aux élèves du premier et du second degré. Pour initier les enseignants et les élèves à ces

thématiques, les institutions publiques ont élaboré des matériaux pédagogiques de premier niveau. VIGINUM et son Académie dédiée à la lutte contre les manipulations de l'information – dont les missions sont rappelées dans le décret n° 2026-70 du 11 février 2026, notamment en matière d'information au public et d'éducation aux médias, en cohérence avec les orientations portées par le Secrétaire général de la défense et de la sécurité nationale et inscrites dans la Stratégie Nationale de lutte contre les manipulations de l'information – a en effet conçu [deux kits de sensibilisation spécifiques](#) publiés en mars 2026, répondant à un besoin de sensibilisation intergénérationnel. Le premier s'adresse directement aux jeunes publics de 10 à 13 ans, transformant les concepts abstraits de manipulation de l'information en activités ludiques adaptées. Le second outille les adultes, parents comme éducateurs, pour comprendre les mêmes notions ainsi que les vecteurs d'ingérence. Ces deux documents peuvent être exploités conjointement en classe avec des supports audio, permettant d'ancrer les propos théoriques dans des formats narratifs proches des usages juvéniles tels que [Le débrief de Clara et Raphaël](#), série de fiction rassemblant huit *podcasts* consacrés aux modes opératoires les plus utilisés dans les diverses campagnes d'ingérences numériques étrangères (INE) : contrefaçon d'opinion ou *similitantisme* (*astroturfing*), infox vidéo, typosquat (*typosquatting*), *copy-pasta*, *trolling*, bulles de filtres, biais et influences algorithmiques.



Le Centre pour l'éducation aux médias et à l'information (CLEMI) offre à cet égard aux enseignants des exemples de séquences pédagogiques structurées. Pour le collège, une approche pertinente consiste à utiliser des documents authentiques liés à des événements d'actualité majeurs tels que les Jeux olympiques et paralympiques de Paris 2024. Lors d'une séquence type, les élèves sont amenés, par groupes, à décortiquer un corpus documentaire de publications en utilisant une grille d'analyse fournie par VIGINUM. L'objectif n'est pas simplement de repérer le faux, mais d'identifier les modes opératoires précis, tels que la manœuvre sous fausse bannière, la décontextualisation de contenus audiovisuels ou la création de contenus générés avec l'IA (► [Fiche pédagogique CLEMI](#)).

Au lycée, la complexité s'accroît avec la réalisation d'une fresque des ingérences numériques étrangères. Ce dispositif collaboratif mobilise un jeu de cartes notionnelles que les élèves doivent articuler logiquement. En cartographiant les acteurs étatiques, non-étatiques et para-étatiques, les vecteurs de diffusion et les impacts sociétaux, les lycéens peuvent acquérir une vision systémique de la guerre de l'information. La séance aboutit en conclusion à la formulation de solutions citoyennes (► [Fiche pédagogique CLEMI](#)). Il est possible par ailleurs de s'appuyer sur la plateforme francophone des initiatives de lutte contre la désinformation (ODIL), qui répertorie un vaste panel d'initiatives francophones de vérification, allant des laboratoires d'analyse africains aux outils d'intelligence artificielle dédiés à la détection de manipulations (► [Ressources pédagogiques](#), [formations](#) ).

31 Éducation aux médias et à l'information

EducARTE, intégré nativement dans le pack de ressources numériques de certains espaces numériques de travail (ENT) régionaux comme la [Normandie](#) met à disposition de tous une fiche thématique intitulée « [Comprendre et déjouer les mécanismes de manipulation de l'information avec VIGINUM](#) » déjà mentionnée dans la [Lettre ÉduNum EMI n°3 \(septembre 2025\)](#) consacrée à l'OSINT. Lumni et Lumni Enseignement publient en ligne des ressources éducatives exploitables en classe, reprenant pour le premier la vidéo pédagogique de la CNIL (► [Utiliser le renseignement en sources ouvertes, ou OSINT, pour la réidentification sur Internet](#) **CNIL**.) et partageant pour le second un lexique de l'IA et des ingérences numériques étrangères (► [IA et ingérences numériques étrangères : le lexique](#) **Lumni**) associé à trois importants dossiers pédagogiques : Élection présidentielle de 2027 : quels risques d'ingérences étrangères en France ? Comment parler des ingérences numériques étrangères en classe ? INE : l'IA au cœur des stratégies de la Russie et de la Chine.



Le projet OSINT4Fun, continuité du calendrier de l'avent de l'OSINT mis en place en 2023 par Céline Girardeau et Alain Godon (Université d'Angers) produit et met à disposition des contenus réutilisables sous licence CC BY-NC 4.0 (tutoriels sur les méthodologies et outils d'OSINT, dossiers thématiques, [défis éducatifs et ludiques](#)). À titre d'exemple on pourra s'intéresser au cas de [la symbiose entre le crocodile et le pluvier d'Égypte](#) analysé dans une investigation en lien avec les travaux d'**Agatha Liévin-Bazin**, docteure en éthologie spécialisée dans le comportement social des oiseaux et autrice de *Mytho animaux : stop les intox* (2023). La longue enquête est menée dans une première partie à partir des résultats des moteurs de recherche puis dans une seconde en exploitant les articles scientifiques.



Luc Viatour, CC BY-SA 3.0
[Wikimedia Commons](#)

Se former : parcours Magistère « Désinformation et ingérences numériques étrangères »

Le parcours de formation [Désinformation et ingérences numériques étrangères](#) a été coconstruit par le CLEMI et VIGINUM à destination des enseignants. Il concentre trois grands objectifs : définir les ingérences numériques étrangères et catégoriser les modes opératoires, découvrir les techniques de détection d'une ingérence numérique étrangère et analyser des séances de classes consacrées aux ingérences numériques étrangères.



D'une durée d'environ 1h30 ce parcours permet notamment de comprendre et d'utiliser une typologie des ingérences numériques étrangères en mobilisant un vocabulaire spécifique, de découvrir comment la thématique des ingérences numériques étrangères peut être abordée en classe avec des élèves de quatrième et de première et d'identifier les liens entre cette thématique et les programmes d'enseignement moral et civique (EMC) ainsi que d'éducation aux médias et à l'information (EMI).

La vision par ordinateur en tant que dispositif de surveillance

La vidéosurveillance algorithmique (VSA) dans l'espace public

Politique de sécurité et vidéosurveillance

Les dispositifs technologiques de vidéosurveillance connaissent un vif succès dans le domaine privé mais aussi public. Plusieurs villes françaises, notamment dans le sud-est, ont intégré ces dispositifs dans leur politique locale de sécurité. Mais à ce jour, aucun décompte exhaustif des dispositifs de vidéoprotection n'est établi malgré des mises à jour régulières, et même si certaines communes n'hésitent pas à communiquer sur le sujet (► [franceinfo](https://franceinfo.fr)).

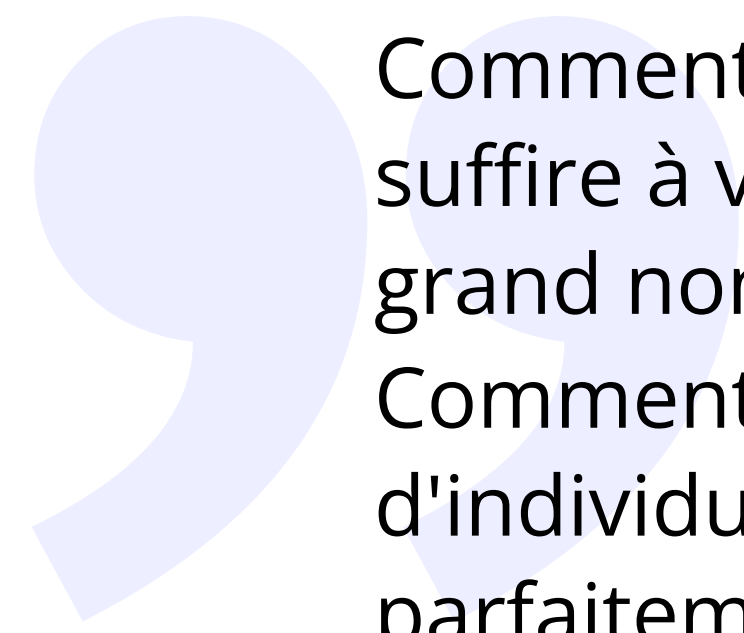


FARRUGIA, Clément, 2024. *La carte de France des villes sous vidéosurveillance*. data.gouv.fr [en ligne]. 2024. [Consulté le 8 mai 2026]. Disponible à l'adresse : <https://www.data.gouv.fr/reuses/la-carte-de-france-des-villes-sous-videosurveillance>

Par exemple, la [plaquette](#) de la police municipale de la commune des Pennes-Mirabeau indique que « dans ce domaine, notre ville [les Pennes-Mirabeau] est également en avance puisqu'on compte 1 caméra pour 86 habitants contre 1 caméra pour 553 habitants à Marseille. Ce qui place les Pennes-Mirabeau au niveau de Nice, commune ayant le plus de caméras par habitant, parmi les grandes villes françaises ». Le critère de la vidéosurveillance permet à une commune de 22 500 habitants de rivaliser avec des communes plus grandes, comme Marseille (environ 900 000 habitants) ou Nice (environ 360 000 habitants). Aucune mesure fiable de l'acceptation par la population de ce type de dispositif n'a été publiée à ce jour. Pourtant, ces dispositifs de surveillance des populations font l'objet d'une promotion des politiques de sécurité de certaines communes.

La VSA pour répondre au problème de Bentham

Un dispositif de vidéosurveillance nécessite des caméras, un centre des opérations (le centre de supervision urbain, ou CSU) et des opérateurs (agents de surveillance des voies publiques, ou AVSP). Mais au-delà d'un certain nombre d'écrans, l'œil humain atteint ses limites. Faudrait-il encore plus d'yeux ? Si oui, dans quelle mesure ? Nous rencontrons alors le problème de la surveillance énoncé dans le *Mémoire* que **Jeremy Bentham** fait parvenir à **Garran de Coulon** (*Panoptique. Mémoire sur un nouveau principe pour construire des maisons d'inspection, et nommément des maisons de force*, 1791. [Gallica](#). p.4) :



Comment un homme seul peut-il suffire à veiller parfaitement sur un grand nombre d'individus ? Comment même un grand nombre d'individus pourrait-il veiller parfaitement sur un seul homme ? Si l'on admet, comme il le faut bien, une succession de personnes qui se relaient, il n'y a plus d'unité dans leur instruction, ni de suite dans leur méthode.

— *Jeremy Bentham*

Est-il possible de rationaliser les coûts de la surveillance tout en maintenant une haute exigence d'efficacité ? Pourrait-on se passer de l'œil humain pour surveiller ? Le logiciel BriefCam (► [Caméras augmentées](#) - CNIL) propose une analyse algorithmique des images. On appelle cela la vidéosurveillance algorithmique, ou VSA : « dernier arrivé parmi les outils technologiques au service de la sécurité des Pennois : le logiciel d'intelligence artificielle « BriefCam » », peut-on lire dans la plaquette susmentionnée. « Un outil parfaitement complémentaire à la vidéoprotection puisqu'il permet d'effectuer des recherches précises en un temps record, à partir de divers critères : taille, similitude d'apparence, véhicule, plaque d'immatriculation, nature et couleur de vêtement... Les opérateurs peuvent ainsi analyser des heures de captures vidéo en quelques minutes et ainsi identifier précisément les personnes et les objets d'intérêt ». Implantés dans l'espace public, les dispositifs de vidéosurveillance sans algorithme impliquaient un certain nombre d'opérateurs, c'est-à-dire des yeux humains scrutant des images sur des écrans et des personnes évaluant des situations. Plus il y avait d'images, plus il fallait d'ASVP. L'assistance algorithmique de la vision par ordinateur permet d'augmenter le nombre d'images analysées sans augmenter le nombre d'opérateurs ASVP, c'est-à-dire sans augmenter le nombre d'images vues et analysées par des humains.

La solution VSA et son cortège de difficultés

Mais est-ce encore l'opérateur qui analyse les images ? Qui analyse l'image ? Qui voit l'image analysée ? Personne ? Serait-il possible de surveiller sans voir ? Les dispositifs de VSA, de plus en plus répandus dans les politiques locales de sécurité, interrogent le législateur en mettant en question la frontière entre le public et le privé. La CNIL est mobilisée en garde-fou des usages possibles de ces analyses d'images (► [Caméras et autres dispositifs vidéo](#)) Différentes interrogations émergent qui peuvent dépasser le cadre de la fiabilité du dispositif. Dans le juridique, une municipalité a-t-elle le droit de procéder à l'analyse algorithmique de toutes les images ? Si cela est permis pour certaines images seulement, qu'ont-elles de si spécifiques par rapport aux autres ? Dans le judiciaire, le résultat d'une analyse algorithmique d'images peut-il servir à l'instruction d'un dossier ? Elles ouvrent finalement sur des perspectives éthiques : comment encadrer la puissance de surveillance d'un tel dispositif ? En 2020, la mairie de Nice, installe un dispositif de surveillance VSA autour de 144 écoles. La CNIL demande l'arrêt de ce dispositif et en janvier 2026, le Conseil d'État s'aligne sur les préconisations de la commission nationale de l'informatique et des libertés en imposant à la municipalité son blocage.

« Voir », « reconnaître » et « apprendre »

À l'origine de ces interrogations se trouve une certaine compréhension de ce qu'on appelle « voir », « reconnaître », « apprendre » lorsqu'on parle de vidéosurveillance algorithmique.

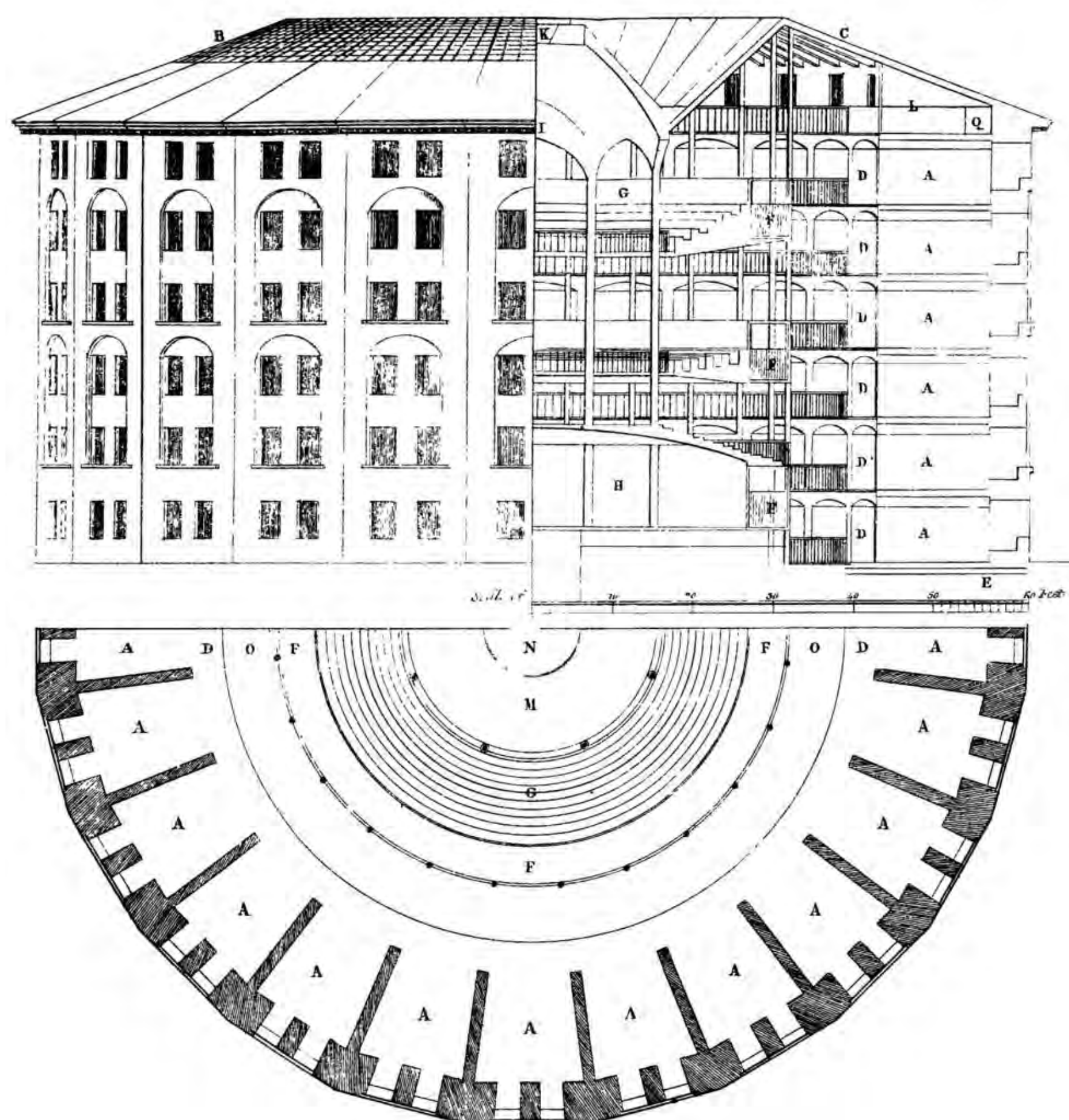
Le dispositif VSA repose sur une technologie du domaine de l'IA qui s'appelle la « vision par ordinateur ». Dès lors, une question très simple se pose : a-t-on besoin d'un œil humain pour surveiller des humains ? Quel sens sommes-nous prêts à donner à l'expression « vision par ordinateur » ? Notre langage ordinaire réalise des raccourcis parfois trompeurs. Dans l'expression « vision par ordinateur », les termes « vision » et « ordinateur » sont si proches qu'on peut finir par dire qu'un ordinateur voit. Pourtant, un logiciel de reconnaissance d'images, réalisant par exemple la tâche « reconnaître les images de chat », ne voit et ne reconnaît jamais le chat de l'image de chat qu'il « reconnaît ». Notre manière ordinaire de parler des dispositifs technologiques d'IA a tendance à faire de ces dispositifs des agents (► [Appréhender le fonctionnement des IA génératives](#), académie de Montpellier) pour mieux les penser. Notamment, lorsqu'on parlera d'apprentissage machine (*machine learning*) à propos de la vision par ordinateur, on entendra dire que l'ordinateur « a appris » à « reconnaître » des chats. Or, ce qui a lieu dans ce dispositif n'a rien d'un agent : il s'agit d'une suite mathématiquement ordonnée d'activations électroniques de semi-conducteurs. Pourtant, dans le cas de la « vision par ordinateur », cédant à une illusion du langage ordinaire, on peut finir par dire, et peut-être même souvent par croire, que « la machine voit le chat de l'image » ou que « la machine reconnaît le chat sur l'image » ou que « l'ordinateur a appris à reconnaître des chats ».

Panoptique et VSA : deux dispositifs de surveillance des populations

Le modèle panoptique : la fiction surveillante

La VSA apporte une nouvelle solution au problème que pose Jeremy Bentham. Il en avait lui-même proposé une selon un modèle architectural d'un bâtiment appelé le Panoptique. L'intérêt du Panoptique est défini par le principe utilitariste :

- il augmente l'efficacité de la surveillance tout en en diminuant le coût : les effets de surveillance sont permanents et ne nécessitent qu'un très petit nombre de surveillants ;
- il moralise les comportements humains en comptant sur les effets de surveillance que les surveillés exercent en permanence sur eux-mêmes en raison d'un potentiel permanent de visibilité : « être incessamment sous les yeux d'un inspecteur, c'est perdre en effet la puissance de faire le mal, et presque la pensée de le vouloir ».¹²



Jeremy Bentham. *Panopticon*, [Wikimedia Commons](#)

¹² Le but du Panopticon consiste en une amélioration morale des prisons et des conditions de vie qui sont décrites ainsi dans le mémoire : « les prisons ont été jusqu'à présent un séjour infect et horrible, école de tous les crimes et entassement de toutes les misères ». Le dispositif de surveillance panoptique cherchait à se donner les moyens matériels d'une moralisation des détenus mais également des surveillants pénitentiaires, conformément au principe général du plus grand bonheur. Cette architecture aux effets moralisants et éducatifs pouvait ensuite s'étendre aux hôpitaux, aux écoles, aux manufactures (cf. Lettre I des *Panopticon letters* dans *Panopticon writings* établis par Bozovic).

Quelle distinction faire entre le dispositif de surveillance et la surveillance tout court ? Dans le dispositif de surveillance de Bentham, il y a une identité entre le surveillant et le surveillé

alors que sans le dispositif, il y a une différence entre le surveillant et le surveillé : l'un surveille, l'autre est surveillé. Dans le cas du Panoptique, c'est par un certain arrangement de l'espace que chaque surveillé produit la fiction du surveillant omniprésent. On doit le Panoptique à l'art de l'architecture et à une compréhension précise de ce que signifie pour un être humain la potentialité d'être vu. Les propriétés du dispositif de surveillance découlent de sa configuration matérielle, non des agents humains de la surveillance. Dans l'architecture panoptique, il s'agit de la circularité du bâtiment composée des cellules, de l'ouverture des cellules vers le centre du cercle, toutes offertes à la vue depuis la tour d'inspection placée au centre du cercle, elle-même disposant d'une jalousie permettant au surveillant de voir en un coup d'œil sans être vu (► Lettre II des *Panopticon letters*). On parle alors d'effets de surveillance. La structure architecturale du Panoptique suffit pour engendrer en chacun la conscience d'être un surveillé en puissance, sans jamais pouvoir savoir quand il en est un en acte. Il n'est nul besoin d'un agent de la surveillance pour engendrer des effets de surveillance et modifier les comportements, notamment les contenir. Les effets de surveillance découlent d'une visibilité des corps élaborée par un certain agencement de l'espace. Les humains modifient leur comportement, non en fonction de la présence effective d'un surveillant dans la tour de contrôle, mais en maintenant la fiction. Afin de décrire le panoptique, **Miran Bozovic** articule une ontologie de la fiction à une ontologie carcérale dont le principe exclut d'un lieu toute expérience possible de la réalité :

”

(...) moins l'inspecteur est réellement présent, plus il est apparemment omniprésent ; ou, plus précisément, l'inspecteur est apparemment omniprésent dans la stricte mesure où il n'est pas réellement présent puisque son exposition momentanée aux yeux des prisonniers est suffisante pour lui faire perdre son apparente omniprésence. Ici, par conséquent, l'apparence exclut la réalité.

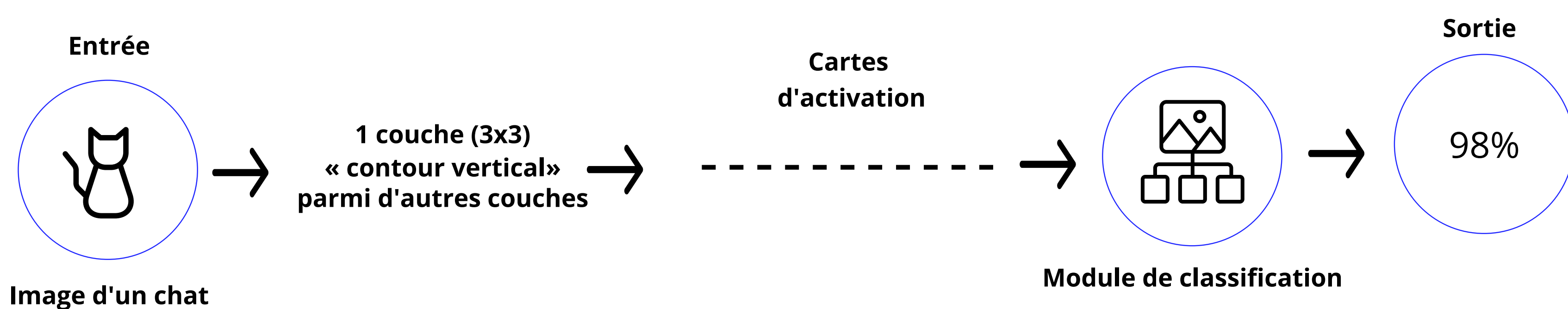
– Bozovic, *Jeremy Bentham, The Panopticon writings, Introduction, p. 9 (traduction de Nicolas Pellet)*

Dans l'espace carcéral matériellement déterminé du Panoptique, il n'y a aucune place pour la réalité de la surveillance. La conscience d'être vu à *tel* moment, à *tel* endroit, en train de faire *ceci* brise l'apparente universalité de la surveillance. La surveillance universelle, en tout temps, en tout lieu, ne se maintient que par la fiction de l'omni-surveillant alors que la particularité d'une surveillance actuelle réduirait les effets de cette fiction à néant. Paradoxe ontologique : seule la conservation d'un être en puissance a des effets ; la seule potentialité de l'être-vu induit des comportements contenus, retenus, voire empêchés par le surveillé lui-même. Les effets de surveillance ne proviennent pas du dispositif architectural. Le seul agent de la surveillance dans le Panoptique idéal décrit par Bozovic, c'est le surveillé lui-même. Mais sans l'arrangement de l'espace panoptique, une telle agentivité du surveillé serait impossible. Il faut donc pouvoir décrire le dispositif pour comprendre les effets de surveillance qu'il rend possibles.

Une description du dispositif de surveillance VSA : le ConvNet

Le dispositif de surveillance VSA est un dispositif essentiellement électronique. L'empreinte du dispositif dans l'espace public est minimale : des caméras, parfois des indications sur les frontières des zones concernées. La présence d'une caméra suppose un champ et donc aussi un hors champ. L'œil de la caméra n'est pas l'œil omniscient du surveillant fictif du Panoptique. La technologie s'appelle ConvNet, abréviation consacrée pour « réseaux

neuronaux convolutifs ». Cette structure électronique proposée pour la première fois dans les années 1980 par **Yann LeCun** s'inspire des travaux de deux neuroscientifiques **David Hubel** et **Torsten Wiesel** portant sur le système visuel des primates, du *cognitron* de **Kunihiko Fukushima** ainsi que sur l'approche constructiviste de Piaget dans le domaine de l'apprentissage. Les ConvNets sont « *la* force motrice de l'actuelle révolution dans la vision par ordinateur et dans d'autres domaines », écrit **Melanie Mitchell** (Mitchell, 2023, p.78). Elle rend possible un accroissement conséquent du nombre d'images analysées. On y trouve une entrée (mettons une image pixelisée d'un chat), une série de cartes d'activation multicouches, un module de classification et une sortie (un indice de confiance, c'est-à-dire une probabilité). On obtient le schéma suivant :



De la gauche vers la droite : du simple au complexe

Ce schéma peut se lire de la gauche vers la droite, c'est-à-dire de l'entrée vers la sortie. Chaque couche des cartes d'activation associe un nombre à une section de pixels de plus en plus petite. Dans notre exemple, la section de pixels sera de 3 x 3, soit un carré de 9 pixels¹³. Chaque couche est affectée à une section. Ce nombre est associé à la section en fonction de la brillance et de la couleur des pixels. Chaque couche a une caractéristique dédiée. Par exemple, une couche dédiée à la caractéristique « contour droit vertical » affectera un grand nombre à telle section de pixels si ceux-ci brillent de sorte à séparer la section en deux régions selon une ligne verticale. Le nombre sera très petit dans le cas contraire.

¹³ Pour avoir un ordre de grandeur, les écrans de faible résolution, comme ceux des ordinateurs portables d'entrée de gamme, sont composés de plus de 1 million de pixels, plus de 3,5 millions pour les écrans de haute résolution. L'écran d'un smartphone est composé de plus de 2 millions de pixels.

... Net

Les couches des cartes d'activation sont dites plus ou moins profondes. Cela veut dire qu'il y a plus ou moins de couches pour une carte d'activation, jusqu'à des centaines de couches pour une carte d'activation et autant de cartes d'activation peuvent composer le ConvNet. Le mot « profondeur » signifie le nombre de couches par carte. De la gauche vers la droite, une carte d'activation en activant une autre, les caractéristiques gagnent en finesse et en complexité : d'une première décomposition de l'image d'entrée jusqu'à des carrés de pixels très petits comme dans notre exemple de couche « contour vertical » 3 x 3. On comprend mieux le Net (réseau) de *ConvNet*. L'architecture est un réseau de cartes qui sont elles-mêmes des réseaux de couches.

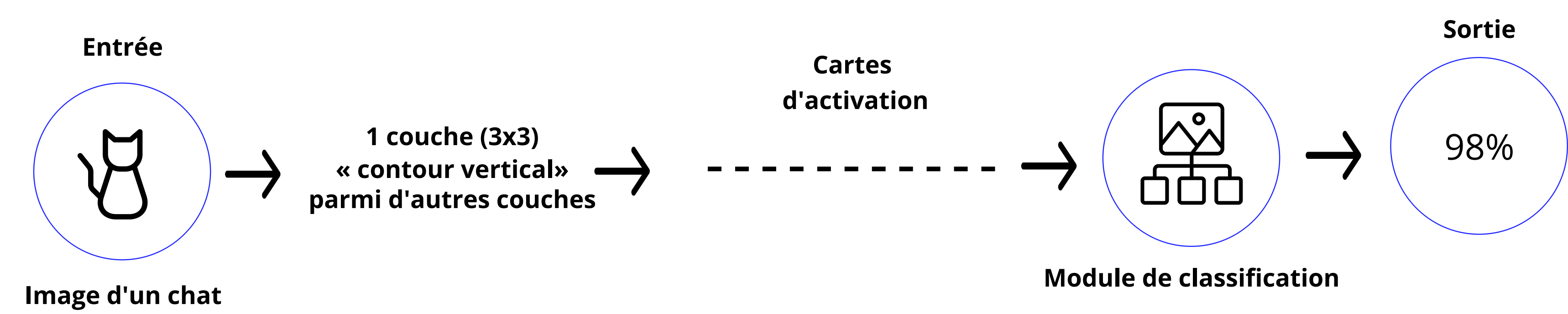
Conv...

Il reste à comprendre le *Conv* qui est l'abréviation de convolution. La convolution est un calcul qui consiste à multiplier la valeur de chaque pixel par son poids et ensuite à additionner chaque valeur de la section. Cela donne la valeur d'activation de la couche. Plus la valeur d'activation est élevée, plus il est probable que la section contienne la caractéristique dédiée à cette couche. Le poids est déterminé de telle sorte à donner la plus forte activation possible quand la caractéristique dédiée est présente.

ConvNet

Ci-dessous une mise en forme de cette architecture et le calcul du nombre d'activation d'une couche de la première carte. Pour notre exemple, la section de l'image par couche

est de 3x3, c'est-à-dire un carré de 9 pixels. Le poids des pixels correspondant à cette couche est établi pour déterminer la présence d'une ligne verticale sur la colonne de gauche de la section. Le nombre associé à chaque pixel par la couche est compris entre 0 et 255 par convention (chaque pixel est codé en trois couleurs selon le [système RVB](#)) :



La couche 3x3, « contour vertical » : (250, 110, 50 ; 190, 100, 20 ; 170, 30, 10) – les coordonnées se lisent ainsi : pixel de la ligne du haut : 250, 110, 50 ; pixels de la ligne médiane : 190, 100, 20 ; pixels de la ligne du bas : 170, 30, 10 ; le pixel en haut à gauche de la section est celui qui brille le plus avec la valeur 250 ; celui en bas à droite est celui qui brille le moins avec la valeur 10. La ligne verticale droite est la moins brillante avec les valeurs 50, 20, 10 alors que la ligne verticale gauche est très brillante avec les valeurs 250, 190, 170.

Notre carré de pixels 3x3 peut se représenter ainsi :

250	110	50
190	100	20
170	30	10

Les poids de notre carré de pixels sont les suivants : (1, 0, -1 ; 1, 0, -1 ; 1, 0, -1). Afin de détecter une ligne droite verticale à gauche de la section, les poids des pixels de la colonne de gauche sont à 1; les autres sont plus petits.

On obtient la table de poids suivante :

1	0	-1
1	0	-1
1	0	-1

Ce qui donne la convolution suivante :

250 x 1

110 x 0

50 x -1

190 x 1

100 x 0

20 x -1

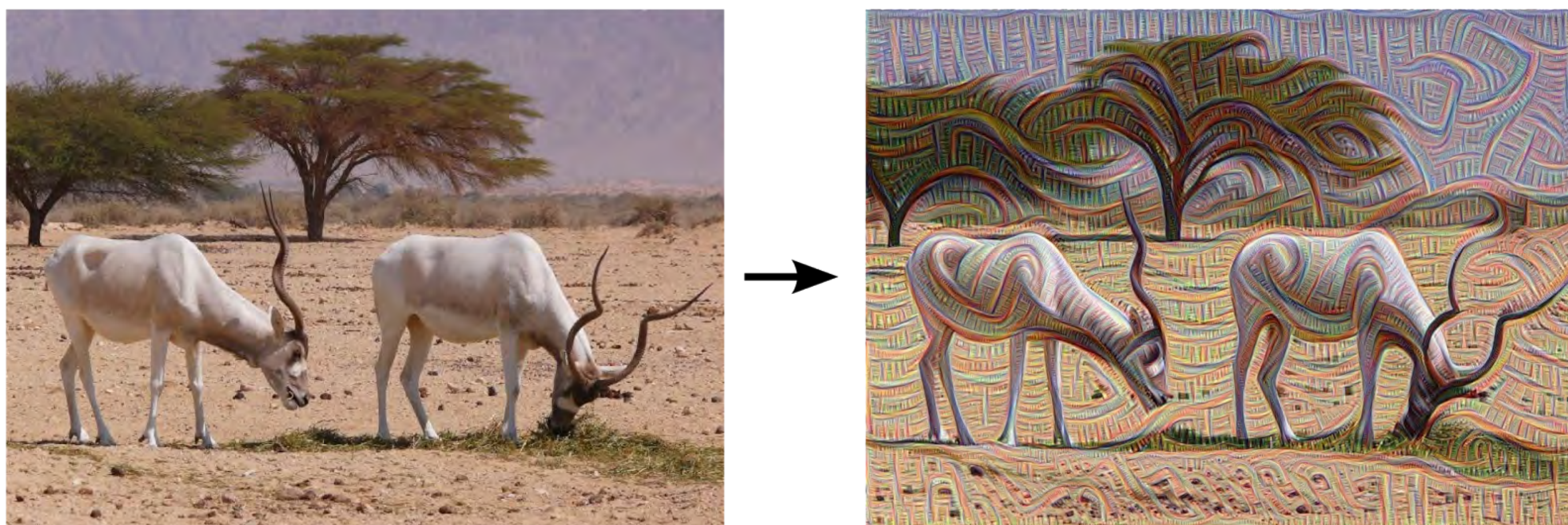
170 x 1

30 x 0

10 x -1

Somme : 530

Dans notre exemple, le nombre d'activation de la couche est élevé. En effet, le nombre maximal d'activation de cette couche est 765. (quand tous les pixels de la ligne verticale gauche sont à 255 et tous les autres à 0, soit 255×3). 530 est donc plutôt un nombre élevé. Selon le résultat des autres couches, qui s'occuperont des autres sections de l'image, et des autres cartes, qui s'occuperont d'autres caractéristiques, chaque carte s'activera selon un certain niveau d'activation (► Mitchell, 2023, « Deuxième partie. Regarder et voir » et la note 1 du chapitre 2 sur la fonction sigmoïde appliquée aux résultats de chaque couche. Il s'agit d'un théorème mathématique appelé théorème d'approximation universelle). Le module de classification reçoit en entrée les activations des cartes et, selon les caractéristiques qui déterminent dans notre exemple la présence d'un chat dans une image, il met en forme un calcul d'indice de confiance.

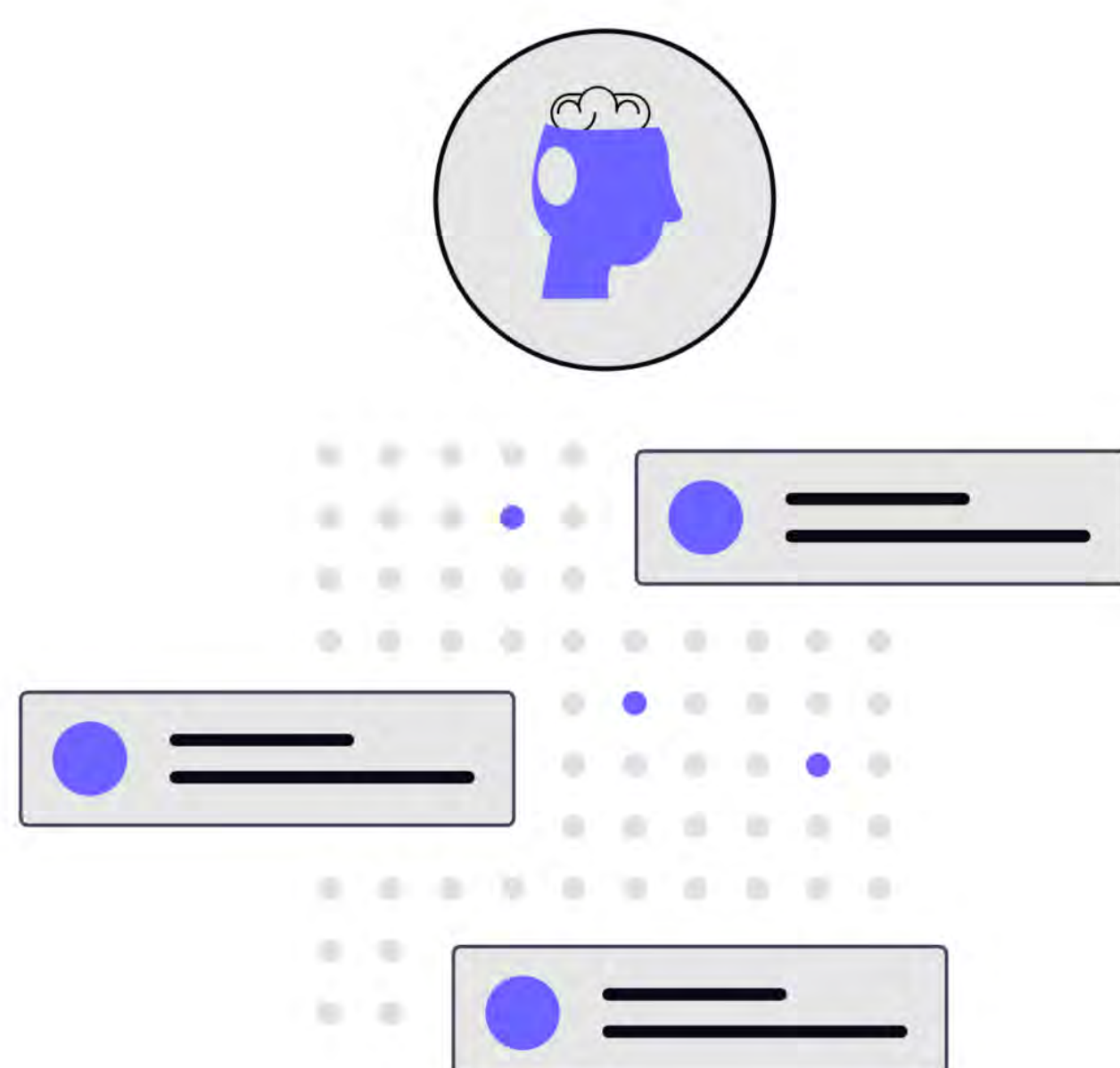


Zachi Evenor, Günther Noack, CC BY-SA 3.0, <https://creativecommons.org/licenses/by-sa/3.0/>, [Wikimedia Commons](#)

De la droite vers la gauche : rétropropagation selon la pente de l'erreur

Le schéma peut aussi se lire de la droite vers la gauche. Ce sens de lecture est mis en forme par l'algorithme de rétropropagation d'où provient l'expression « apprentissage machine ». Il s'agit de confier au ConvNet le soin de la configuration des poids de chaque couche. Pour cela, il faudra commencer par constituer un fichier d'images de chat, images parfaitement étiquetées. À chaque erreur de « reconnaissance », un outil mathématique permet de remonter la pente de l'erreur jusqu'à certains poids qui seront alors modifiés automatiquement en fonction de la pente (► Algorithme du gradient. Cf. ouvrage gratuit sous licence Creative Commons BY-NC de **Michael Nielsen**, [Neural Network and deep Learning](#)). L'apprentissage machine consiste en un réglage automatisé des poids du ConvNet.

Au bout d'un certain temps d'ajustement des poids, le ConvNet fera de moins en moins varier les poids. On appelle cela une époque d'apprentissage. Le test avec de nouvelles images peut alors commencer. Si le test n'est pas concluant, il faudra recommencer avec un fichier d'images correctement étiquetées, peut-être plus large, affiner la pente d'erreur, de nouvelles époques, etc.



« Voir », « reconnaître » et « apprendre » dans le dispositif VSA

« Voir » et « reconnaître »

Que voit un ordinateur ? Que reconnaît-il ? À strictement parler, rien. Ce qu'on dit être vu par vision algorithmique n'est pas identifié en une unité visuelle synthétique subjective par les différents éléments électroniques mobilisés par le dispositif. Il n'est pas non plus identifié en une unité conceptuelle synthétique objective par l'agglomération de différentes caractéristiques, pourtant très nombreuses. Il manque ce que Kant appelle le « troisième terme » (► Kant, *Critique de la raison pure* – Du schématisme des concepts purs de l'entendement, trad. Alquié, La Pléiade, Gallimard, p.885) , c'est-à-dire le schème, terme hybride, « homogène d'un côté à la catégorie, de l'autre au phénomène », qui est la condition qui rend possible l'application du concept au phénomène.

Kant écrit :

« Le concept de chien signifie une règle d'après laquelle mon imagination peut tracer de manière générale la figure d'un quadrupède, sans être restreinte à quelque figure particulière que m'offre l'expérience, ou encore à quelque image possible que je peux présenter in concreto. » (p.887).

Reconnaître un chien quand on en voit un suppose une liberté de l'imagination. Si elle était soumise aux cas particuliers de chien, chaque cas particulier de chien, avec sa singularité de couleur, de taille, de poils, de position, de comportement, etc. nous empêcherait d'étendre le concept de chien d'un cas particulier à un autre. Or, c'est bien ce qu'on fait quand on reconnaît ce qu'on voit. Malgré toutes les différences et la variabilité des cas particuliers de chiens, nous sommes capables d'affirmer ou de nier « chien » de la réalité que nous voyons. Le schème suppose la liberté de l'imagination relativement aux particularités des cas. Cette liberté implique une règle qui ne dérive pas des cas particuliers. Quelle est cette règle ? D'où vient-elle ? Ni une image, ni un concept, cette règle, écrit Kant, est « un art caché dans les profondeurs de l'âme humaine, et dont nous aurons de la peine à arracher à la nature les secrets du fonctionnement pour les mettre à découvert sous nos yeux » (p.887).

Reconnaître un chien quand on en voit un suppose un jugement affirmant l'unité objective de la chose vue sans se fonder sur les particularités de ce chien. Cette affirmation suppose qu'une règle a été suivie puisque nous parvenons à appliquer un concept général de chien à un cas particulier de chien. Mais si cette règle est donnée par les catégories, cette règle se trouve dans « *la nature* », « dans les profondeurs de l'âme humaine », c'est-à-dire qu'elle suppose une unité subjective animée, donc vivante, qui juge. Ce qui conduit le ConvNet à dire qu'il y a très probablement là un chat sur la photo, c'est une série de changements d'états électroniques de beaucoup de semi-conducteurs, série ordonnée selon des fonctions mathématiques explicitées. Le ConvNet est soumis aux différents états électroniques de la matière (► [Cahiers ÉduNum Thématiques n°28, Matérialités](#)) et à des règles de calcul explicites. Ce n'est pas une subjectivité libre, vivante, affirmant ou niant selon une règle qu'elle doit pouvoir trouver en elle sans pouvoir la mettre « sous nos yeux ». Il manque donc à notre ConvNet la faculté de juger. Melanie Mitchell écrit :

« Voici une mise en garde qui vous surprendra peut-être. Lorsqu'un humain dit qu'une photo contient, disons, un chien, nous supposons que c'est parce qu'il voit effectivement un chien sur la photo. Mais si un ConvNet dit « chien », comment savons-nous qu'il fonde sa classification sur le chien de la photo ? Peut-être la photo contient-elle autre chose – une balle de tennis, un frisbee,

une chaussure mordillée – qui étaient souvent associée aux chiens dans les images d'apprentissage, et lorsque le ConvNet reconnaît ces choses, il suppose qu'il y a un chien sur la photo. Ce type de corrélations finit souvent par tromper les ordinateurs. » (p.104).

Complétons cette mise en garde en disant que ce qui vaut pour le chien de la photo vaut également pour les éléments « balle de tennis », « frisbee », « chaussure mordillée » : comment savons-nous que le ConvNet fonde sa classification sur ces différents éléments de la photo ? Bien sûr, il arrive à l'humain de se tromper sur ce qu'il reconnaît. Mais se trompe-t-il comme peut se tromper un ConvNet ? Là encore, il ne faudrait pas tomber dans une illusion du langage car il n'est pas si clair qu'un ConvNet puisse se tromper comme nous le verrons plus tard.

« Apprendre »

On doit principalement aux fonctions de rétropropagation ce qu'on appelle « apprentissage machine ». Mais là encore, le vocabulaire peut nous entraîner dans des croyances mystificatrices. Le ConvNet apprend-t-il quelque chose ? Ce qu'on appelle « apprentissage machine » consiste en un réglage automatisé des poids afin de faire faire au ConvNet ce qu'on veut qu'il fasse. Le nombre de poids à régler augmente très vite. Supposons des sections d'images pixelisées de 5x5, c'est-à-dire 25 pixels. À chaque section correspondrait donc un réglage d'une table de poids de 25 poids. Pour une image de 800x625 composée de 500 000 pixels, il y aurait 20 000 tables de poids à régler, en fonction de la caractéristique que l'on souhaite détecter avec chacune d'entre elles, ce qui exigerait beaucoup trop de temps pour un humain, pour autant que cela soit humainement possible. Il arrive bien souvent qu'on associe à l'apprentissage machine l'idée selon laquelle la machine peut apprendre plus rapidement qu'un humain. L'expression « apprentissage machine » agit alors sur nous comme une description mal définie en nous faisant glisser de « réglage automatisé des poids » vers « la machine apprend ». On confond alors la nécessité de l'automatisation du réglage des poids pour le bon fonctionnement du ConvNet avec ce que ne peut pas faire un humain. On confond une étape de la production de l'objet technique avec une lacune de l'être humain.

La VSA et ses opacités

À partir de là, trois formes d'opacité peuvent être distinguées. La première : l'opacité à propos de ce que nous faisons dans un tel dispositif. S'agit-il d'une prévention contre les délits, les incivilités, les agressions ? Ou bien s'agit-il d'une amplification de nos préjugés ? La deuxième : si les formules mathématiques en jeu dans le dispositif sont explicables, les calculs qui en découlent sont-ils entièrement formulables ? Le ConvNet est-il entièrement explicable ? La troisième : qu'a donc « appris » à faire le ConvNet ? Est-on en mesure de bien déterminer l'objet d'apprentissage ? Nous pouvons respectivement mettre en regard de ces trois opacités les trois principes suivants : équité, transparence et maîtrise du tri des images.

Un dispositif de surveillance ou une amplification de nos préjugés ?

C'est le tristement célèbre scandale de l'application Photos de Google en 2015 : l'application de reconnaissance d'image (un ConvNet) avait étiqueté une image de deux Afro-Américains du terme « Gorilles » (► [Numerama](#)). En 2023, Google en était encore à sa solution à court terme consistant à supprimer l'étiquetage « Gorilles » de son système de reconnaissance. Ces biais racistes trouvent leur origine dans les images d'entraînement du ConvNet, non dans le ConvNet. En forçant le trait, disons que si toutes les images d'humains sur lesquelles s'appuie l'entraînement du ConvNet sont des images d'hommes blancs, il est évident que les

corrections des poids suivront une pente d'erreur amplifiant le préjugé raciste. Mais s'agit-il de préjugés dont il faudrait accuser la machine ou bien d'erreurs dérivant de nos préjugés ? Dans son ouvrage déjà cité, Melanie Mitchell fait également référence à la reconnaissance faciale intégrée à certains appareils photos numériques (p.119). Par exemple, un appareil décrit un visage asiatique comme un clignement des yeux. Ces différents cas démontrent qu'un ConvNet peut très vite basculer en amplificateur de nos préjugés : « Kate Crawford, chercheuse chez Microsoft et militante pour l'équité et la transparence en IA, a fait remarquer que l'un des ensembles de données largement utilisés pour former des systèmes de reconnaissance faciale contient 77,5 % de visage masculins et 83,5 % de visages blancs. Ce n'est pas surprenant dans la mesure où les photos sont chargées depuis des sites de recherche d'images en ligne et que les photos proposées sur ces sites sont généralement celles de personnes célèbres ou puissantes, qui sont surtout des hommes blancs (p.120).

A-t-on toujours les capacités de débusquer de tels biais ? En étiquetant « Gorilles » l'image représentant deux Afro-Américains, le ConvNet de Google ne s'est pas trompé au sens où il n'a fait qu'amplifier un préjugé raciste inclus dans la procédure automatisée des réglages des poids. Par conséquent, si nous n'avons pas toujours les capacités de débusquer de tels biais, l'automatisation des analyses d'images depuis un CSU risque de jeter le doute et une suspicion d'inéquité tout à fait légitime. De telles images auraient-elles été moins analysées si le ConvNet n'avait pas « reconnu » un homme noir ? Auraient-elles été plus analysées si le ConvNet n'avait pas « reconnu » un homme blanc ?

L'IA explicable et l'obligation légale de transparence : « montrez vos calculs ! »

Les fonctions mathématiques du ConvNet sont explicables. Mais qu'en est-il des calculs réalisés ? Qui calcule ? Si on laisse à la machine le soin d'effectuer les calculs, il ne faut pas perdre de vue que nous avons affaire à une analogie. Les semi-conducteurs sont disposés de telle sorte que, les électrons circulant, leurs changements d'état électronique allument tels pixels de manière à représenter un nombre identique au résultat qu'aurait donné un humain qui aurait fait le calcul à la main. La disposition des transistors est aux pixels allumés ce que la disposition des nombres sur la feuille de calcul est au résultat. Imaginons qu'on puisse imprimer la série des calculs effectués par un ConvNet. Qu'est-ce que cela nous apporterait ? Une telle documentation permettrait-elle de répondre à l'exigence d'une IA transparente ? Le nombre des calculs serait bien sûr trop grand pour pouvoir être contrôlés par un humain. Autrement dit, une IA explicable dans le domaine de la vision par ordinateur n'est pas encore disponible et la question de savoir comment le ConvNet s'y prend pour arriver au résultat que tel objet se trouve sur cette image reste sans réponse : « Un réseau neuronal convolutif décide quel objet se trouve dans une image en effectuant une série d'opérations mathématiques (des convolutions) se propageant dans de nombreuses couches. Pour un réseau de taille raisonnable, cela peut représenter des milliards d'opérations arithmétiques » (p.121-122). À supposer que nous détenions une telle liste, elle « n'est pas une explication susceptible d'être comprise par un humain » (p.122).

Nous faisons tous l'expérience, plus ou moins quotidiennement, d'un dispositif de surveillance automatisé : ce qu'on appelle les radars, système de surveillance automatisée de la vitesse des véhicules sur des sections de route qui sont clairement indiquées aux conducteurs. Il est tout à fait possible de déterminer précisément ce qui a conduit un radar à se déclencher lors du passage d'un véhicule. La section de la route où a lieu la surveillance est clairement définie. Le calcul de la vitesse est montrable et la règle de déclenchement est complètement explicitée : au-delà de telle vitesse, une photographie du véhicule est prise et pourra servir de base à une verbalisation. Mais dans le cas du dispositif de surveillance VSA,

on ne peut montrer ni les calculs ni les différents états électroniques de la matière qui ont conduit à la « reconnaissance » automatisée. C'est là une grande difficulté compte tenu de l'obligation légale de transparence qui pourrait, dans le cas d'un ConvNet, se résumer à l'injonction que l'enseignant de mathématiques fait à ses élèves et que rappelle Melanie Mitchell : « Montrez-moi vos calculs ! »

L'objet d'apprentissage et la maîtrise du tri des images : le risque permanent d'une inversion ontologique

La technologie ConvNet souffre d'une autre opacité. Qu'a donc « appris » le ConvNet ? Comment être sûr de lui avoir « appris » à faire ce qu'on voulait lui faire faire ? En général, l'objet d'un apprentissage n'est jamais tout à fait clair. Il est très difficile de déterminer ce qu'a appris l'apprenant. Une situation apparemment analogue se retrouve dans l'apprentissage machine et peut également être la source d'un anthropomorphisme. Dans le cas d'un ConvNet, Mitchell pose le problème en se référant à un travail effectué par l'un de ses étudiants (p.117). Son étudiant devait produire un système de reconnaissance d'images permettant de trier entre des photos sur lesquelles il y a un animal et des photos sur lesquelles il n'y en a pas. À la fin de l'entraînement, son système ayant réalisé des tests satisfaisants sur l'échantillonnage d'apprentissage, l'étudiant le teste sur un nouvel échantillonnage d'images et rencontre des erreurs. Ces erreurs ont une explication assez déroutante : le système avait appris à trier entre les images à l'arrière-plan flouté et au premier plan net, non à trier les images d'animaux.

En effet, toutes les images d'apprentissage partageaient cette technique photographique qui consiste à faire la mise au point sur le sujet de la photo. Le ConvNet ne s'était donc pas trompé. S'il avait réussi à trier les images d'animaux, ce n'était que par accident car il triait en réalité tout autre chose. Pour neutraliser un tel biais, il faudrait pouvoir séparer l'objet du tri qu'on souhaite de ce qui vient toujours avec lui, c'est-à-dire séparer, selon la distinction aristotélicienne, la substance (*ousia*) de l'accident (*sumbebekos*). Mais cela est tout simplement impossible. Une telle abstraction ne se trouve pas dans la réalité. La liaison substance/accident est continue et la substance vient toujours avec ses accidents.

L'apprentissage de la reconnaissance d'une chose ne peut donc pas se résumer en une collection d'exemples de cette chose. S'en tenir à une diversité de cas pour établir l'objet d'un tri peut conduire à une inversion cocasse de la substance et de ses accidents, comme dans le cas des arrière-plans floutés. Mais l'inversion peut parfois être dramatique et très grave dans le cas de l'étiquetage « Gorilles » du couple d'Afro-Américains par l'application Photos de Google, qui a inversé l'accident « noir » et la substance « humain ».

Peut-on se contenter de montrer à un enfant un certain nombre de corps rouges pour lui apprendre à reconnaître la couleur rouge ? Non seulement personne ne procède ainsi, mais en procédant ainsi, l'enfant peut tout à fait comprendre autre chose. Il peut comprendre par exemple que le mot « rouge » désigne une certaine forme d'objet, voire tel objet et non sa couleur. Qu'est-ce qu'« apprendre à reconnaître » dans la reconnaissance d'images ? Il s'agit de faire coïncider un terme avec la chose que ce terme désigne. Ni le geste de la monstration d'un corps rouge par l'index accompagné de l'énoncé « c'est rouge », ni la multiplication d'exemples de « rouge » ne supprime le doute sur ce que l'apprenant apprend à reconnaître. Bien au contraire, l'ambiguïté de l'apprentissage y trouve à chaque fois son origine. Une fois qu'on a montré l'objet rouge à l'enfant en lui disant « c'est rouge », qu'a-t-il appris ? A-t-il appris à faire correspondre le terme « rouge » à la couleur ou à autre chose ? Une fois qu'une machine a mis en nombre des millions d'images où la couleur rouge se trouve, qu'a-t-elle mis en nombre exactement ? Comme la couleur n'est jamais séparée

d'un corps, un corps d'une forme, d'une position, etc., en montrant ou en codant des choses de couleur rouge, on montre et on code aussi les corps, leurs formes et de nombreuses autres choses encore.

De la surveillance-*empeiria* à la surveillance-*technè* pour une culture de l'IA

Ces trois lieux d'opacité mettent en jeu la fiabilité et la compatibilité légale du dispositif VSA. Melanie Mitchell rapporte dans son ouvrage une comparaison qu'elle avait effectuée entre un simple *perceptron* sans rétropropagation et un ConvNet avec rétropropagation :

”

[...] j'ai comparé les performances d'un perceptron et d'un réseau neuronal à deux couches, chacun doté de 324 entrées et de 10 sorties, à la reconnaissance de chiffres manuscrits, en entraînant les deux réseaux sur 60 000 échantillons d'apprentissage. J'ai ensuite testé leurs performances sur 10 000 nouveaux échantillons de chiffres. Le perceptron a eu un taux de réussite de 80% sur ces nouveaux échantillons, tandis que le réseau neuronal, avec 50 unités cachées, a connu une réussite faramineuse de 94%. Victoire aux unités cachées ! Mais qu'a exactement appris le réseau neuronal pour dépasser de si loin la performance du perceptron ? Je n'en sais rien. Peut-être pourrais-je trouver un moyen de visualiser les 16 700 poids du réseau neuronal pour me faire une idée des raisons de sa supériorité, mais je n'ai pas essayé, et en général, il n'est pas du tout facile de comprendre comment ces réseaux prennent leurs décisions. (p.41)

– *Melanie Mitchell*

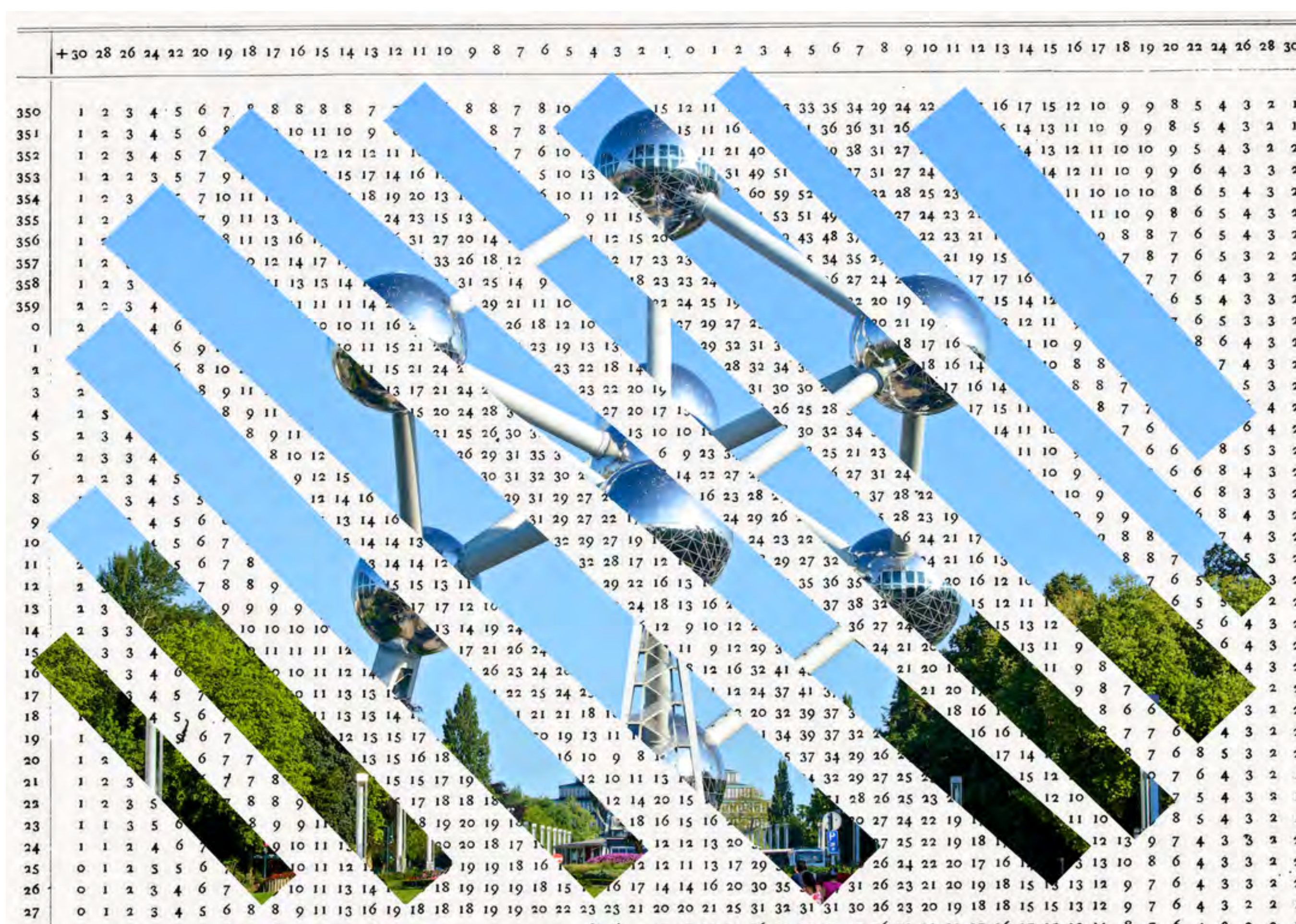
Platon distinguait entre l'activité *technè* et l'activité *empeiria*, que nous traduisons souvent par « technique » et « routine ». L'activité technique est une activité dans laquelle on sait ce qu'on fait, on sait comment on le fait, en vue de quoi on le fait, et, quand on le fait, on sait qu'on le fait. L'activité accomplie par routine est le contraire. Emportés par les habitudes, nous ne savons parfois même plus que nous sommes en train de faire quelque chose. Le dispositif VSA interroge à nouveau cette frontière. Si nous ne savons ni ce qu'a « appris » le ConvNet, ni comment l'analyse d'images se déclenche, ni même si le déclenchement d'une analyse d'images approfondie a lieu, nous sommes dans l'activité *empeiria*, non dans l'activité *technè*. Nos pratiques de surveillance augmentées d'IA sont dès lors à interroger.



ArchaiOptix, Peintre d'Antiphon. CC BY-SA 4.0 [Wikimedia Commons](#)

Le modèle Panoptique répondait au problème de Bentham par des moyens architecturaux en vue d'une réforme morale de la société par l'extension de l'être-vu en puissance à tout l'espace public. Le modèle VSA vise la prévention des incivilités, des délits, des crimes. Pourtant, la présence de ce dispositif dans l'espace urbain est minimale. Les caméras sont difficilement localisables par les gens. La nécessaire limitation du champ de l'objectif de la caméra implique un espace hors-champ et la zone vidéosurveillée doit être explicitement bornée et indiquée.

L'architecture Panoptique était la condition de possibilité des effets de surveillance. Elle maintenait le surveillé dans une agentivité utile, efficace et peu coûteuse : par la fiction du surveillant omniscient, le surveillé devenait son propre surveillant. La technologie ConvNet est entourée d'effets de langage pour en simplifier les descriptions : l'ordinateur « voit », « reconnaît », « apprend ». L'analyse de ces effets de langage nous conduit au mieux à nous interroger à nouveau sur ce que nous-mêmes entendons par « voir », « reconnaître » et « apprendre ».



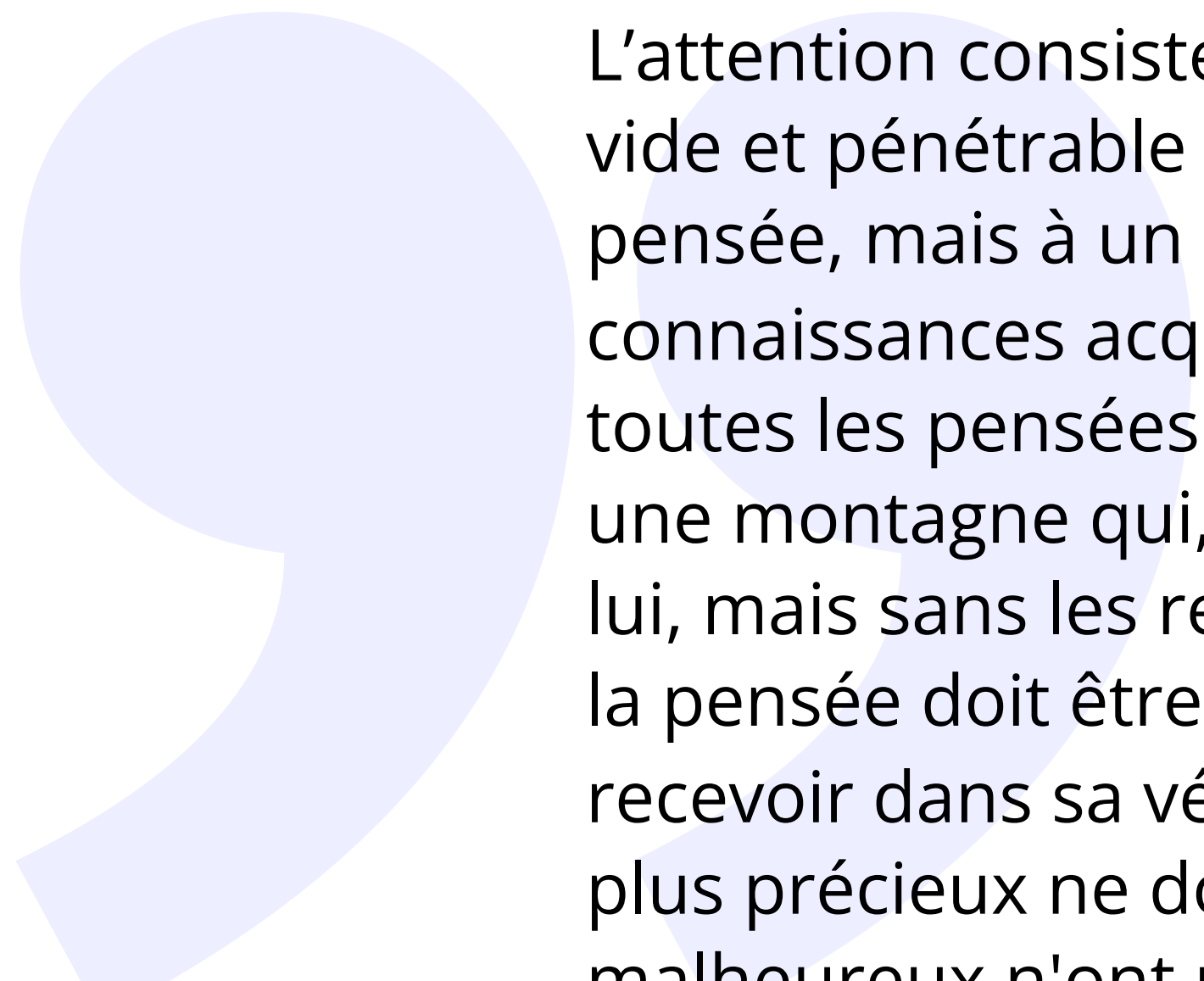
Anna Riepe & FARI / <https://betterimagesofai.org/> / <https://creativecommons.org/licenses/by/4.0/>

La grande quantité des images analysées par les ConvNet peut séduire et sembler utile pour régler les conflits et instruire les dossiers judiciaires. La substitution à la subjectivité humaine de l'opération automatique pourrait donner une impression de gain d'objectivité. Mais les images numériques traitées par le ConvNet impliquent des points d'opacité portant sur l'objet même du dispositif, pour autant qu'il en reste un : ce dispositif est-il un dispositif de surveillance ou d'amplification de nos préjugés ? Savons-nous comment et par quoi ont lieu les analyses de telles images et non des autres ? Le tri des images est-il effectué tel que nous le souhaitons ? Ces interrogations ouvrent une dynamique critique, dont on peut espérer qu'elle permette de passer d'une surveillance-*empeiria* à une surveillance-*technè*, et ainsi de développer une véritable culture de l'IA.

Repenser la surveillance : vers une éthique de la relation

Vigilance et attention

Être vigilant c'est s'emplir des bruits du monde, à la différence de l'attention ; c'est ce que **Simone Weil** explique : être attentif impose une ouverture, une écoute, qui m'oblige à une certaine fermeture envers ce que je n'ai pas choisi d'entendre.



L'attention consiste à suspendre sa pensée, à la laisser disponible, vide et pénétrable à l'objet, maintenir en soi-même à proximité de la pensée, mais à un niveau inférieur et sans contact avec elle, les diverses connaissances acquises qu'on est forcé d'utiliser. La pensée doit être, à toutes les pensées particulières et déjà formées, comme un homme sur une montagne qui, regardant devant lui, aperçoit en même temps sous lui, mais sans les regarder, beaucoup de forêts et de plaines. Et surtout la pensée doit être vide, en attente, ne rien chercher, mais être prête à recevoir dans sa vérité nue, l'objet qui va y pénétrer. (...) Les biens les plus précieux ne doivent pas être cherchés, mais attendus. (...) Les malheureux n'ont pas besoin d'autre chose en ce monde que d'être capables de faire attention à eux. La capacité de faire attention à un malheureux est chose très rare, très difficile ; c'est presque un miracle, c'est un miracle. Presque tous ceux qui croient avoir cette capacité ne l'ont pas. La chaleur, l'élan du cœur ne suffisent pas. (...) Ce regard est d'abord un regard attentif, où l'âme se vide de tout contenu propre pour recevoir en elle-même l'être qu'elle regarde tel qu'il est, dans toute sa vérité. Seul en est capable celui qui est capable d'attention.

— *Simone Weil, Attente de Dieu, 1963, p. 85-97.*

La vigilance envers autrui ne s'appellera pas attention car à lire Simone Weil on aura compris qu'il n'y a place pour aucune dissimulation dans le monde de l'attente. Disponibilité à l'autre, telle est cette ouverture sans *a priori* : une vigilance non attentive qui se pose souvent comme « bienveillante ». Car derrière une disposition affective à l'égard d'autrui se profile une veille, voire une surveillance d'autrui.

La vigilance appartient aussi à l'insensé

Pour éviter de se perdre en chemin, il s'agit de faire usage de cette lumière naturelle dont les hommes pensent être si bien pourvus, qu'ils ne cherchent pas à en avoir plus qu'ils n'en ont : ironie de Descartes à l'encontre de ceux qui sont si peu attentifs envers eux-mêmes qu'ils s'égarent d'abord de leur fait. Cependant, suffit-il d'être éveillé pour ne pas se tromper ? Comment être certain que je ne confonds pas la veille et le rêve ? Car je suis homme, écrit Descartes dans la première de ses *Méditations Métaphysiques*, et à ce titre, il m'arrive de dormir : « Toutefois j'ai ici à considérer que je suis homme, et par conséquent que j'ai coutume de dormir et de me représenter en mes songes les mêmes choses, ou quelquefois de moins vraisemblables, que ces insensés, lorsqu'ils veillent. Combien de fois m'est-il arrivé de songer, la nuit, que j'étais en ce lieu, que j'étais habillé, que j'étais auprès du feu, quoique je fusse tout nu dedans mon lit ? ».

Rêver d'être invisible pour mieux surveiller

Voir sans être vu, c'est accéder à un savoir interdit, un lieu secret. Le rêve de big Brother ? Ce jeu d'espionnage, cette infraction du désir, ce désir de l'omniscience, nous renvoient à la tentation de l'illimité, une tentative de dépassement de soi. On se rappelle peut-être, cette histoire de berger que nous raconte Platon dans le deuxième livre de la *République*. Il a pour

nom Gygès. C'est un homme simple qui obéit aux lois de la Cité, un homme sans histoire, jusqu'au jour où le hasard le met en présence, d'un anneau découvert dans une cavité du sol. Le berger met l'anneau à son doigt et devient invisible après en avoir tourné le chaton. Dès lors il se laisse aller à toutes les turpitudes et à tous les excès. Les autres n'existent plus.



L'anneau de Gygès, huile sur bois du XVIe siècle. Ferrare. [Wikimedia](#)

De la vigilance à la surveillance : se tenir à l'écart de la sensibilité

Avant la Révolution française, l'État affichait sa puissance par des spectacles de cruauté dans l'espace public, mettant en scène la souffrance pour renforcer son autorité. Le théâtre accentuait cette sensibilité, comme l'explique Michel Foucault à propos du dernier écartèlement, illustrant comment le châtement était conçu pour impressionner par sa brutalité. Le panoptique de Jeremy Bentham succède à cette cruauté théâtrale. La rigueur géométrique de ses lignes a aussi pour but d'inscrire la norme dans les corps, mais en le faisant le plus insensiblement possible (► Michel Foucault, *Surveiller et punir*. Le Panoptisme, chapitre III) : « De là, l'effet majeur du Panoptique : induire chez le détenu un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir. Faire que la surveillance soit permanente dans ses effets, même si elle est discontinue dans son action ; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice ; que cet appareil architectural soit une machine à créer et à soutenir un rapport de pouvoir indépendant de celui qui l'exerce ; en bref que les détenus soient pris dans une situation de pouvoir dont ils sont eux-mêmes les porteurs ».

Giorgio Agamben prolonge cette analyse en expliquant que le dispositif d'exclusion radicale, dont les camps de concentration seront la figure, est au contraire de rendre invisible : « Il faut réfléchir au statut paradoxal du camp en tant qu'espace d'exception :

c'est un bout de territoire qui est placé en dehors du système juridique normal, mais qui, pour autant, n'est pas simplement un espace extérieur. Ce qui exclut en lui est, selon le sens étymologique du terme exception (ex capere), pris au dehors, inclus grâce à leur exclusion même. Mais ce qui, de cette façon, est avant tout capturé dans le système, c'est l'état d'exception lui-même. Le camp est la structure dans laquelle se réalise durablement l'état d'exception. **Hannah Arendt** a remarqué autrefois que dans les camps apparaît très clairement le principe qui régit la domination totalitaire et que le sens commun se refuse obstinément à admettre, c'est-à-dire le principe selon lequel « tout est possible ». Parce que les camps constituent, dans le sens que l'on a vu, un espace d'exception où la loi est intégralement suspendue, tout y est vraiment possible. (Giorgio Agamben, extrait de « Qu'est-ce qu'un camp ? », in *Moyens sans fins, notes sur la politique*, 2002).

Prendre soin d'autrui dans sa vulnérabilité

L'individualité est constituée de façon intersubjective, et la vulnérabilité des individus réside dans l'exposition à l'autre. Invitation est faite de repenser la lutte pour la reconnaissance de Hegel (► Kim Sang Ong-Van-Cung, 2010. [Reconnaissance et vulnérabilité Honneth et Butler](#). *Archives de philosophie*, 119-141 ; [La vulnérabilité est-elle une faiblesse ?](#), 2022. *radiofrance*, Sommes-nous tous vulnérables?). Dans un livre très important pour la philosophie morale et politique contemporaine, *Un monde vulnérable*, la philosophe américaine **Joan Tronto**, que l'on considère comme l'une des principales contributrices du courant des éthiques du *care* (ou du soin), écrit : « La vulnérabilité a d'importantes conséquences morales. Elle apporte un démenti au mythe selon lequel nous serions des citoyens toujours autonomes et potentiellement égaux. Supposer l'égalité entre les humains laisse de côté d'importantes dimensions de l'existence Joan Tronto montre ainsi que le *care* en tant que réparation nous sort de l'impossible « égalité » pour les femmes et de l'aporie des concepts politiques (► Joan C. Tronto, 2009. *Un monde vulnérable : pour une politique du care*).

Manière d'ouvrir, pour la surveillance, à une bien-veillance de l'attention et de la vigilance, celles de l'infirmière au chevet du malade, celles de la mère au berceau de l'enfant, celles du professeur auprès de l'élève, d'autres horizons que ceux qui les réduisent, avec l'industrie numérique, les données massives et les technologiques d'intelligence artificielle, à des matières premières, à des produits industriels et des marchandises, ou à des modes d'assujettissement des populations.

Laissons la conclusion à Simone Weil qui sut si bien retenir notre attention, pour se prêter « à recevoir dans sa vérité nue » ce qui est à côté de moi.

Le nouveau chronomètre. La surveillance numérique au travail

Dans le salariat contemporain, la surveillance n'est pas une anomalie. En droit français, le lien de subordination se caractérise notamment par le pouvoir de l'employeur de diriger le travail et d'en contrôler l'exécution. Ce pouvoir répond aussi à ses responsabilités en matière d'organisation et de sécurité. Les technologies numériques paraissent toutefois inaugurer une ère inédite du contrôle. Des *webcams* et des logiciels vérifient la présence des télétravailleurs à leur poste ; des *GPS* suivent les déplacements des livreurs ; des logiciels de sécurité scrutent les courriels des salariés sous couvert de protéger l'entreprise ; dans les entrepôts de la grande distribution, chaque geste de l'ouvrier est chronométré par le scanner qui lui dicte où aller et quoi prélever. Une part croissante des travailleurs exerce aujourd'hui sous le regard continu de dispositifs numériques qui enregistrent, mesurent et évaluent leur activité.

Le projet qui anime ces dispositifs est pourtant ancien de plus d'un siècle. Lorsque **Frederick Winslow Taylor** formule les principes de l'organisation scientifique du travail en 1911, il fait déjà de la surveillance la clé de voûte du management. Rendre le travail visible pour le connaître, le connaître pour le prescrire, le prescrire pour le contrôler. Les technologies numériques ne créent pas cette logique ; elles la prolongent, l'approfondissent et l'automatisent, en levant une à une les contraintes matérielles qui limitaient jusque-là la surveillance : elle était intermittente, car nul contremaître ne pouvait tout voir en permanence ; elle exigeait la présence physique du surveillant auprès du surveillé ; et elle s'arrêtait aux portes de l'atelier ou du bureau. On définira la surveillance numérique comme toute collecte et tout traitement systématique de données, facilités par les technologies numériques, portant sur des informations identifiables ou anonymisées, dans l'intention explicite ou implicite d'influencer, de gérer ou d'évaluer les individus dans un contexte de travail (Gonzalez Vazquez et al., 2025). Deux éléments méritent d'être soulignés. D'abord, la nécessité d'un traitement : toute collecte ne constitue pas en soi une surveillance ; encore faut-il que les données recueillies soient analysées. Ensuite, la relation de pouvoir : ces données analysées doivent être mobilisées pour agir sur ceux qu'elles ciblent. C'est cette finalité (influencer, gérer, évaluer) qui distingue la surveillance de la simple production de traces numériques et l'inscrit dans une logique de pouvoir. Cette réflexion se propose d'examiner une double transformation : ce que le numérique change à la surveillance au travail et, en retour, ce que cette surveillance transformée change au travail lui-même. Une question guidera tout le parcours : ce que la technique rend possible, les organisations le font-elles ? Autrement dit, la surveillance numérique se déploie-t-elle partout où elle le peut, ou quelque chose en décide-t-il autrement ?

L'analyse porte principalement sur l'emploi salarié ordinaire, en Europe et en Amérique du Nord, où le phénomène est le mieux documenté. Le cas des travailleurs des plateformes numériques de type Uber, abondamment étudié par ailleurs, est laissé de côté. Ce choix permet de montrer que la surveillance numérique, souvent poussée à son terme dans l'économie des plateformes, est également présente dans l'emploi salarié ordinaire. Elle se déroulera en cinq temps. On reviendra d'abord sur la matrice taylorienne, où la surveillance apparaît comme instrument de connaissance et de contrôle. On décrira ensuite l'extension des capacités de surveillance dans le temps et dans l'espace, par la diversification de ses acteurs et par l'approfondissement de ce qu'elle observe, puis ses effets sur les conditions de travail. On s'interrogera enfin sur l'ampleur réelle et inégale du phénomène et sur les filtres juridiques, managériaux et collectifs qui en règlent le déploiement.

Ce propos permet enfin de relire le questionnement de terminale « Quelles mutations du travail et de l'emploi ? », qu'il aborde sous un angle inhabituel : celui de la surveillance, prise comme fil conducteur pour revisiter les modèles d'organisation du travail et leurs effets sur les conditions de travail.

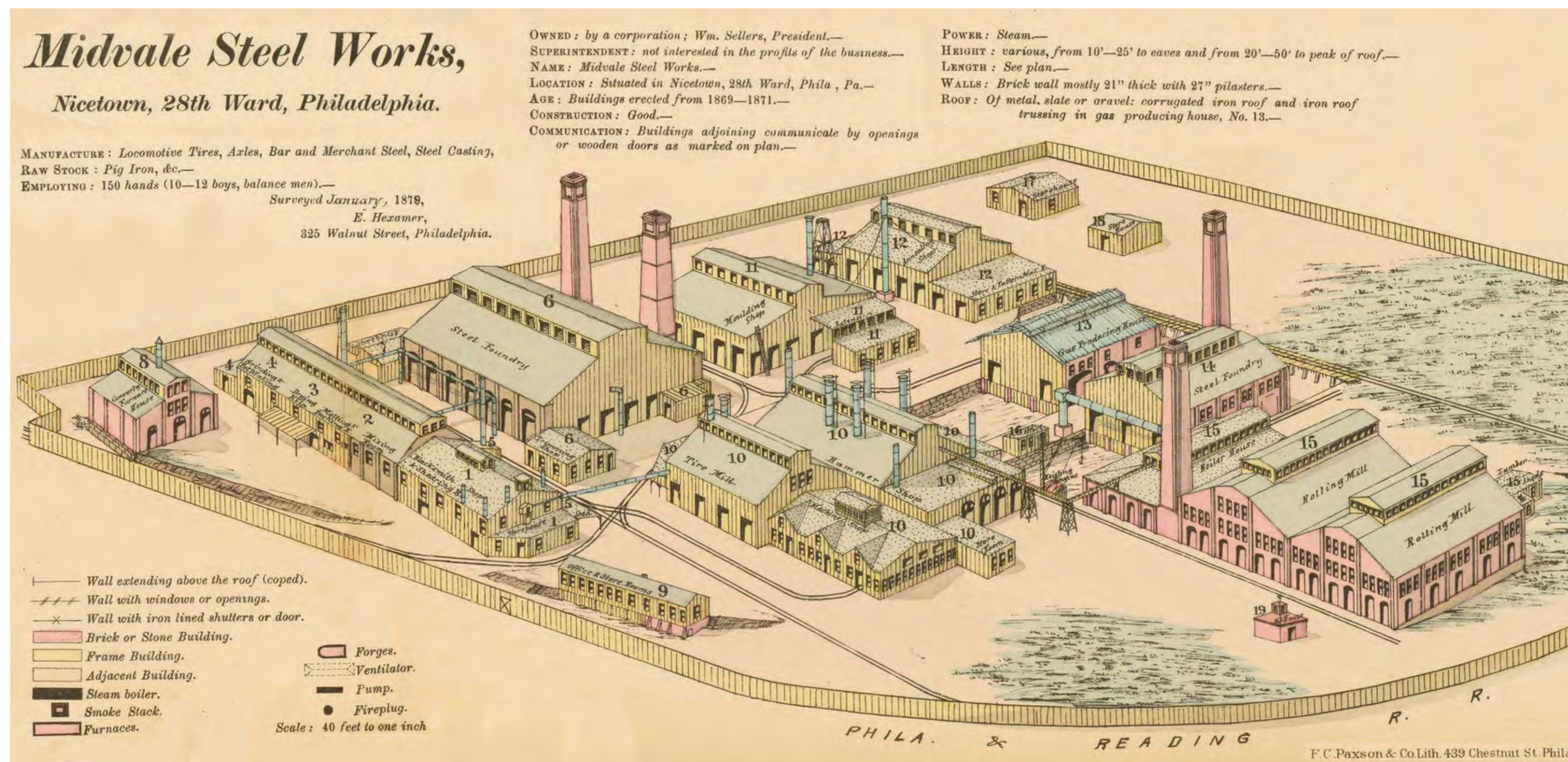
La surveillance au travail dans l'organisation scientifique du travail

De l'organisation scientifique du travail, on retient d'ordinaire la division du travail, la parcellisation des gestes et la stricte relation hiérarchique : c'est ainsi qu'elle s'enseigne, et c'est exact. Olivier Aïm (2020) qui ouvre ce cahier ÉduNum, invite pourtant à relire *Les principes de l'organisation scientifique du travail* (1911) sous un autre angle. Il en fait l'un des textes pionniers des théories de la surveillance (voir infra) : chez Taylor, la surveillance n'est pas un accessoire du système, elle en est l'un des fondements, à la fois condition de la connaissance du travail et instrument de son contrôle. C'est cette relecture que suit la présente section. Elle permettra de saisir ce que les dispositifs numériques actuels doivent à la matrice taylorienne et ce qu'ils y ajoutent. Le diagnostic de Taylor repose sur deux constats. Le premier est l'ignorance des directions : dans le système ancien, le savoir-faire appartient aux ouvriers, qui ont appris leur métier par observation et transmission orale, et Taylor observe dans chaque métier une multitude de méthodes, « quarante, cinquante ou une centaine de façons différentes » d'accomplir une même tâche. La direction ignore le travail réel qui s'effectue dans ses ateliers, et ce qu'elle ne connaît pas, elle ne peut ni le prescrire, ni le mesurer, ni l'améliorer. Le second constat est celui de la « flânerie ».

Structurées dans les années 1980 et 1990, les *Surveillance Studies* constituent un champ interdisciplinaire qui étudie comment les institutions et les organisations recueillent et traitent des informations sur les individus afin de les gérer ou de les contrôler. Ce champ puise dans un héritage théorique plus ancien, du panoptique de Bentham à l'analyse foucaldienne du pouvoir disciplinaire, et a développé ses propres concepts pour saisir les formes contemporaines de surveillance fondées sur les données. Olivier Aïm (2020) en propose une synthèse en français.

À la flânerie naturelle, tendance humaine à économiser ses efforts, s'ajoute une flânerie systématique : les ouvriers ralentissent volontairement leur cadence tout en donnant l'impression de travailler au maximum de leurs capacités, par peur du chômage ou parce que les incitations salariales sont mal conçues. Cette résistance constitue pour Taylor un obstacle majeur, car elle est difficilement observable : contrairement au gaspillage de matières premières, les « gestes humains maladroits, inefficaces, ou mal supervisés ne laissent aucune trace visible ou tangible derrière eux ». La perte de rendement se loge dans ce qui échappe au regard. Ces deux problèmes appellent une même réponse : la surveillance. Celle-ci remplit une double fonction. Elle est d'abord un instrument de *connaissance* : par les études de temps au chronomètre, la décomposition des mouvements, les fiches et les archives, la direction extrait le savoir ouvrier, le transforme en données, en standards, en « lois ». Elle est ensuite un instrument de *contrôle* : ce savoir une fois codifié, il

s'agit de « suivre de près chaque homme, pour s'assurer que le travail est bien fait suivant les principes posés ». Taylor rationalise la surveillance elle-même : dans les ateliers de la



Hexamer, *Midvale Steel Works Aerial View*, 1879. Image recadrée et réagencée. [Wikimedia](#)

Midvale Steel Co – compagnie sidérurgique de Pennsylvanie où Taylor mena, entre 1898 et 1901, les expériences qui nourrissent les *Principles of Scientific Management* – l'unique contremaître d'autrefois est remplacé par huit hommes aux fonctions spécialisées, de l'inspecteur au responsable de la discipline. C'est, selon la formule d'Aïm, une véritable « division du travail appliquée à la surveillance » : le regard porté sur l'ouvrier est lui-même décomposé, spécialisé, optimisé, exactement comme les gestes qu'il observe. Lui-même enregistre la plainte des ouvriers découvrant ce système : « Eh bien quoi, je ne peux même plus penser ou bouger sans que quelqu'un le fasse pour moi ou me dise comment faire ! » L'ouvrier est désormais placé « sous observation constante » en un double sens : objet d'une étude scientifique continue et d'une inspection permanente de la conformité de son travail. Rien de ce que révèle cette observation ne se perd : les performances quotidiennes de chaque ouvrier sont notées et archivées, constituant une mémoire écrite du travail que la direction peut consulter et comparer à tout moment. Il n'y manque que la base de données. Un siècle plus tard, la logique n'a pas changé ; les moyens, si. C'est cette extension des capacités de surveillance qu'il s'agit maintenant de décrire.

L'extension des capacités de surveillance

Taylor voulait placer l'ouvrier sous observation constante, mais cette surveillance reposait sur des moyens humains, outillés de quelques instruments rudimentaires comme le chronomètre. Or l'observation humaine est coûteuse et nécessairement discontinue : elle mobilise des personnels dédiés, ne peut tout couvrir à la fois et laisse subsister de nombreux angles morts. La visibilité totale du travail demeurerait ainsi un idéal que les instruments de l'époque ne permettaient pas d'atteindre. Le numérique lève ces contraintes en mettant le travail en données. Chaque geste, chaque déplacement, chaque échange laisse désormais une trace quantifiée, que l'organisation peut stocker, comparer et analyser : de quoi connaître le travail, et contrôler ceux qui l'accomplissent, à un degré dont Taylor n'aurait pas rêvé. Cette extension emprunte cinq directions principales, que les développements suivants illustreront. La présente section décrit donc ce que les dispositifs permettent ; ce que les entreprises en font, et pourquoi, occupera les sections subséquentes.

Extension de la surveillance	Ce que le numérique rend possible
Continue et automatisée	L'activité de travail produit elle-même des données, automatiquement et sans interruption. Cadences, pauses et erreurs peuvent être suivies en temps réel.
Hors les murs	Le déroulement du travail devient visible à distance, au moyen des smartphones, applications de suivi et outils de télétravail.
Distribuée	L'évaluation n'est plus réservée au manager : clients et collègues y participent par les notes, enquêtes et outils collaboratifs.
Plus profonde	Le suivi ne porte plus seulement sur l'activité observable, mais sur les émotions, le stress, la fatigue ou la santé, inférés à partir des textes, de la voix ou du corps.
Prédictive	Les données passées et présentes sont utilisées pour anticiper les départs, les performances, les promotions ou les comportements jugés problématiques.

Une surveillance continue et automatisée

Les entrepôts logistiques de la grande distribution et du *e-commerce* illustrent la continuité et l'automatisation de la surveillance. Depuis les années 1990, les technologies numériques y ont accompagné un vaste mouvement de rationalisation et d'industrialisation du travail, faisant des entrepôts de véritables « usines à colis » (Benvegnù et Gaborieau, 2020). Dans ces entrepôts, le préparateur de commandes passe sa journée à parcourir de longues allées pour rassembler les articles d'une commande. Guidé par un scanner portable ou par un casque à commande vocale relié au logiciel de gestion de l'entrepôt, il reçoit ses instructions en continu : un emplacement, une référence, une quantité. Selon les sites, il conduit un transpalette sur lequel il empile les articles prélevés sur une palette, ou il avance en poussant un chariot de préparation garni de bacs. À chaque emplacement, il prélève le produit, le scanne ou confirme oralement le prélèvement, puis reçoit aussitôt la consigne suivante. L'opération se répète des centaines de fois par jour, à une cadence imposée et sur des distances pouvant atteindre plusieurs kilomètres. Or chacun de ces gestes laisse une trace. Les dispositifs numériques ne se contentent pas de prescrire le travail, en dictant l'emplacement, l'article et l'ordre des prélèvements ; ils l'enregistrent dans le même mouvement. C'est la double capacité que **Shoshana Zuboff** (1988) a nommée *automate / informate* : en numérisant une tâche, la technologie informatique produit simultanément de l'information sur la façon dont cette tâche s'accomplit. Le même scanner qui indique à l'opérateur quel article saisir consigne l'heure, la durée et la cadence de chaque prélèvement. Il en résulte un déplacement décisif par rapport au dispositif taylorien : la surveillance ne repose plus sur la présence physique de contremaîtres. Là où Taylor devait poster huit hommes pour quadriller l'atelier, la donnée est désormais produite par l'activité elle-même, automatiquement et sans interruption. L'observation cesse d'être un acte distinct ; elle devient un sous-produit continu du travail.

Ces données alimentent une multitude d'indicateurs que le manager peut suivre en temps réel : nombre de commandes préparées, taux de prélèvement, durée des pauses, distances parcourues, nombre d'erreurs, temps consacré à chaque tâche (Gautié et Perez, 2023). La visibilité gagne même le temps improductif, accomplissant un objectif au cœur du projet

taylorien : éliminer les temps morts et traquer la flânerie. Cette flânerie se lit désormais en creux, comme un « temps hors tâche », chaque pause, chaque déplacement non prévu, chaque échange avec un collègue apparaissant comme un blanc dans le flux des données. Dans ces entrepôts au moins, le rêve d'une visibilité sans reste se trouve accompli.

Une surveillance hors les murs

La surveillance du travail n'a jamais été totalement confinée au lieu de production : le travailleur itinérant rendait des comptes, le représentant remontait ses ventes. Mais le contraste restait net entre le dedans et le dehors. Dans l'usine ou le bureau, le contrôle était direct : les contremaîtres et les cadres observaient les salariés et vérifiaient l'exécution des tâches. Hors les murs, il demeurait indirect, différé et lacunaire : l'employeur connaissait les résultats du travail, non son déroulement. C'est cette asymétrie que les dispositifs numériques peuvent abolir. Cette évolution est bien illustrée par les technologies de gestion des travailleurs mobiles, analysées par **Wolfie Christl** (2024). Les techniciens de maintenance itinérants disposaient traditionnellement d'une forte autonomie : responsables de certains sites, ils organisaient leur travail comme ils l'entendaient, hors de portée du regard de leur direction. Le *smartphone* change la donne. Le salarié doit y renseigner chaque étape de sa journée, du départ vers le client à l'achèvement de chaque tâche, si bien que son parcours et son emploi du temps deviennent visibles sans même qu'une géolocalisation permanente soit nécessaire : la succession des traces suffit. Au siège, une carte numérique permet de savoir en temps réel qui travaille sur quoi.

La même logique gagne les services à la personne, où elle rencontre une difficulté propre : le travail des aides à domicile consiste en tâches relationnelles et domestiques dont le résultat est peu observable. Les applications de suivi y servent précisément à « documenter l'invisible », en enregistrant la localisation, les activités effectuées et le temps qui leur est consacré, afin de prouver que la prestation a bien eu lieu. Justifiée par la facturation et le contrôle du service rendu, cette traçabilité ouvre la voie à un contrôle plus étroit : les durées réelles des visites sont comparées aux durées contractuelles, et les écarts systématiques repérés. Le travail hors de l'entreprise, que l'employeur ne connaissait jadis que par les comptes rendus, devient ainsi une donnée enregistrée et évaluable.

La surveillance suit aussi le salarié en télétravail, jusqu'au domicile. Ce contrôle prend deux formes. La première repose sur des logiciels spécialisés qui enregistrent les frappes au clavier et prennent à intervalles réguliers des captures d'écran, quand ils ne permettent pas de revoir l'intégralité des actions effectuées sur le poste. L'objectif est de reconstituer à distance une image aussi précise que possible de l'activité réelle, et surtout de débusquer tout signe d'inactivité. Ces logiciels se sont surtout diffusés en Amérique du Nord, dans des contextes juridiques qui les entravent peu. Ils ne sont pas absents du paysage français, mais ils s'y heurtent au droit : fin 2024, la CNIL a sanctionné une entreprise qui surveillait ses télétravailleurs au moyen d'un logiciel décomptant leurs « temps d'inactivité », mesurés par l'absence de frappe ou de mouvement de souris, et prenant des captures d'écran régulières¹⁴. Leur usage reste toutefois marginal en Europe (voir infra).

La seconde tient aux outils de télétravail eux-mêmes, qui deviennent des instruments de suivi. Visioconférences, messageries et agendas partagés rendent d'abord visibles les disponibilités, les temps de connexion et les sollicitations : de quoi vérifier qu'un salarié est joignable. Mais l'étude de Meyer et al. (2022) sur le secteur bancaire montre que l'essentiel se joue ailleurs. Contrairement à ce qu'on aurait pu attendre, le contrôle par les résultats

¹⁴ Commission nationale de l'informatique et des libertés (CNIL), formation restreinte, Délibération n° SAN-2024-021 du 19 décembre 2024.

s'est pas renforcé ; ce sont les comportements qui ont été surveillés à distance, par la multiplication des réunions et des points de suivi, par les demandes de partage d'écran, par les sollicitations hors des horaires habituels. Surtout, les salariés se sont mis à se contrôler eux-mêmes : parce que l'entreprise leur fait confiance en les laissant travailler chez eux, ils estiment devoir prouver qu'ils travaillent, acceptent une réunion tardive, répondent le soir, prolongent leur journée. La norme n'est pas édictée, elle est déduite, et le collectif y contribue autant que la hiérarchie. Le salarié devient ainsi en partie son propre surveillant, dans une hyper-disponibilité qui brouille la frontière entre vie professionnelle et vie privée.

Une surveillance distribuée : le client et le collègue comme évaluateurs

Chacun en a fait l'expérience : après un passage chez le garagiste, un courriel invite à remplir un rapide questionnaire de satisfaction ; après un appel au service client, un SMS demande de noter la qualité de l'échange ; après une livraison de colis, un message invite le client à dire comment celle-ci s'est déroulée. Ces sollicitations, devenues routinières, paraissent porter sur la qualité du service. Mais derrière l'enseigne, c'est souvent un salarié identifié qui est noté : les réponses sont rattachées à son dossier, agrégées en indicateurs, consultées par son encadrement. Le client devient ainsi, souvent sans le savoir, un auxiliaire de la surveillance managériale. Ce mécanisme a reçu un nom : on parle de *surveillance réfractive*¹⁵ pour désigner ces configurations où la surveillance du travailleur ne passe pas par un dispositif braqué sur lui, les données collectées auprès des clients étant « réfractées » vers les salariés pour évaluer leur travail. Dans les services mobiles, Christl (2024) montre ainsi que des logiciels de gestion d'interventions calculent un taux moyen de satisfaction client par salarié, à partir des enquêtes envoyées après chaque passage d'un technicien. Le regard du client devient une ressource managériale : il permet de comparer les salariés, de repérer des écarts, d'orienter les discussions sur la qualité du service. Le contrôle en est d'autant plus difficile à saisir qu'il passe par des dispositifs ordinaires, avis, étoiles et notes, devenus outils d'évaluation professionnelle.

¹⁵ L'expression est empruntée à Levy et Barocas (2018) : [Refractive Surveillance: Monitoring Customers to Manage Workers](#)

Cette évaluation par les clients place en outre les travailleurs dans une relation profondément asymétrique (Baiocco et al., 2022). Contrairement au manager, dont l'évaluation s'inscrit dans une relation de travail encadrée par des règles, le client intervient comme un évaluateur externe et ponctuel, dont les critères restent implicites : il peut attribuer une note faible sans tenir compte des contraintes réelles de la prestation, puis disparaître, quand le travailleur en supporte les effets durables. Kellogg et al. (2020) soulignent que ces évaluations externes sont difficiles à comprendre et à contester, reposant sur des critères hétérogènes et intervenant parfois à distance de la prestation.

S'y ajoute un second problème : le regard du consommateur n'est pas neutre (Christl, 2024). Les notes et commentaires peuvent incorporer des stéréotypes liés au genre, à l'origine supposée, à l'âge, à l'accent ou à l'apparence physique. Le jugement du client se présente comme une simple opinion de consommateur ; intégré aux dispositifs numériques de suivi de la qualité, il devient une contrainte professionnelle difficilement réversible. Les travailleurs ne subissent d'ailleurs pas ce dispositif sans l'appriivoiser. Chacun a entendu un livreur ou un conseiller demander explicitement une bonne note, voire préciser le barème : « mettez 10, un 8 me pénalise », le barème ne comptant souvent que les notes maximales. D'autres choisissent leur évaluateur, sollicitant personnellement le client quand l'échange s'est bien passé. La parade ne suspend pas la *surveillance réfractive* ; elle en épouse les règles pour en amortir les effets.

Le regard qui évalue ne vient pas seulement de l'extérieur : il se distribue aussi latéralement,

entre collègues. L'enquête de **Clément Pouré** (2025) en donne une illustration avec le cas de Pierre, développeur dans une *start-up* parisienne. Les outils qu'utilise son équipe rendent l'activité de chacun visible par tous : GitHub affiche le nombre de lignes de code écrites ou modifiées par chaque collègue, Jira suit l'avancement des tâches en cours. « J'ai accès aux statistiques de toute l'équipe », résume Pierre. La comparaison s'impose alors d'elle-même : depuis le début de la semaine, un collègue a réalisé 19 opérations ; lui, « seulement » 14. Et ce « seulement », qu'il prononce lui-même, dit assez que le classement est intériorisé. Or ces outils n'ont pas été conçus pour surveiller : ils servent d'abord à coordonner le travail. Mais en rendant l'activité observable en continu, ils font de tout collègue un témoin et un point de comparaison permanent. La surveillance n'a plus besoin d'être exercée pour être opérante : il suffit que chacun sache que les autres peuvent voir. Les collègues deviennent, comme le suggère le titre de l'enquête, les nouveaux contremaîtres les uns des autres.

Une surveillance plus profonde

Le numérique permet de porter un regard plus profond sur le travailleur. Il ne surveille pas seulement son activité visible (ses gestes, ses horaires, ses déplacements ou sa productivité), mais cherche aussi à saisir des dimensions plus intimes : émotions, stress, fatigue, état de santé ou bien-être. C'est précisément ce que souligne **Ifeoma Ajunwa** (2023) : le management contemporain prolonge le taylorisme, mais en l'étendant bien au-delà du geste productif. Des dimensions jusque-là difficiles à observer ou à objectiver sont désormais traduites en données ou en indicateurs. On s'arrêtera ici sur l'analyse émotionnelle des communications, qui prétend détecter les affects et les états psychologiques des salariés. Les techniques d'analyse des sentiments illustrent ce déplacement du contrôle vers l'intériorité du travailleur : elles visent à transformer les affects exprimés dans les communications professionnelles en données exploitables par l'organisation (Ball, 2021). Issues du traitement automatique du langage, elles déterminent la tonalité émotionnelle d'un message (positive, négative ou neutre) et, dans leurs versions les plus fines, cherchent à identifier des émotions plus précises comme la frustration, la colère, l'inquiétude ou l'enthousiasme. Ces outils ne « lisent » toutefois pas les émotions : ils les infèrent.

Pour qu'un algorithme attribue un sentiment à un texte, il faut d'abord lui apprendre à reconnaître ce qu'est un message positif ou négatif. C'est le principe de l'apprentissage supervisé : on fournit au modèle des milliers d'exemples déjà étiquetés par des humains, avis ou commentaires classés « positif », « négatif » ou « neutre ». En les comparant, le modèle repère des régularités entre certains mots, certaines tournures et l'étiquette correspondante, puis les applique à des textes nouveaux en leur attribuant un score de probabilité : un message pourra être classé comme ayant 82 % de chances d'exprimer une tonalité négative. Le sentiment n'est donc ni lu ni compris par la machine : il est inféré, avec une marge d'erreur, à partir de ressemblances avec des exemples passés.

Un premier usage de ces outils consiste à suivre le climat interne de l'entreprise (Kellogg et al., 2020). Les directions et les services de ressources humaines peuvent les mobiliser pour analyser les réponses aux enquêtes internes, les commentaires laissés sur des plateformes collaboratives ou, plus largement, toute trace écrite produite dans l'organisation. L'objectif affiché est de repérer des tensions, de mesurer l'adhésion à une transformation organisationnelle ou d'évaluer le moral des équipes : l'analyse des sentiments se présente alors comme un outil de pilotage collectif, capable d'objectiver des perceptions jusqu'alors difficiles à saisir. Cette surveillance des communications risque toutefois de fausser ce

qu'elle prétend mesurer. Sachant leurs messages potentiellement analysés, les salariés communiquent avec davantage de prudence : ils évitent les critiques, taisent leurs désaccords et adoptent un langage neutre, conforme aux attentes supposées de l'organisation (Christl, 2024). L'analyse du climat interne ne mesure alors plus ce que les travailleurs pensent, mais ce qu'ils acceptent d'exprimer dans un espace perçu comme surveillé. La surveillance produit elle-même l'appauvrissement des données qu'elle exploite : au lieu de révéler le climat social, elle encourage l'autocensure et masque les problèmes réels.

Un second usage, plus intrusif, concerne le suivi individualisé du travailleur, en particulier dans les métiers de la relation client. Les centres d'appels en sont l'exemple le plus révélateur, comme le montre une enquête récente du *Monde* (Coromines, 2025). Les salariés y font depuis longtemps l'objet d'une surveillance numérique intensive : durée et nombre d'appels, temps de pause, respect du script, taux de résolution ou satisfaction client. L'IA permet désormais d'analyser des aspects plus qualitatifs de cette parole : le ton, l'empathie, l'agacement ou encore le « sourire dans la voix ». Chaque conversation peut être enregistrée, transcrite puis analysée à deux niveaux : ce qui est dit (respect du script, formules d'empathie, mots associés à l'irritation ou à la satisfaction) et la manière de le dire (intonation, débit, silences, tension vocale). À partir de ces indices, le logiciel produit des indicateurs de sentiment, de stress ou de qualité relationnelle, que le manager peut mobiliser pour évaluer la performance, repérer les salariés qui s'écartent des attentes et orienter le suivi individuel : entretiens, formation, rappels à l'ordre, voire mesures disciplinaires.

Mais ces techniques ne sont pas toujours fiables. Les émotions ne se laissent pas aisément réduire à des indices mesurables : une même phrase peut exprimer des affects très différents selon le contexte. L'énoncé « Super ! Encore une réunion ! » peut être lu littéralement comme une marque d'enthousiasme, alors qu'il relève tout aussi bien de l'ironie. De même, une intonation, un accent ou une fatigue passagère peuvent être mal interprétés. Le problème est d'autant plus sérieux que ces évaluations alimentent le management quotidien : comme le souligne **Kirstie Ball** (2021), des inférences fragiles peuvent produire des effets bien réels sur les travailleurs. En Europe, ces dispositifs se heurtent d'ailleurs à un obstacle plus radical que leurs limites techniques : depuis février 2025, le droit européen¹⁶ interdit d'inférer les émotions des travailleurs sur leur lieu de travail, hors raisons médicales ou de sécurité. L'interdiction ne vise toutefois que les systèmes fondés sur des données biométriques : l'analyse de la voix des téléopérateurs y tombe, l'analyse des textes écrits y échappe. Ailleurs, aux États-Unis notamment, rien ne s'y oppose. L'analyse des sentiments scrute l'intériorité affective du salarié à travers ses mots et sa voix. Le même mouvement gagne le corps et la santé : aux États-Unis surtout, des programmes de bien-être adossés à des objets connectés font remonter à l'entreprise l'activité physique, le sommeil ou le rythme cardiaque de ses salariés, sous couvert de prévention¹⁷. Mais la surveillance en profondeur ne s'arrête pas au présent : elle prétend aussi anticiper les comportements futurs.

La surveillance prédictive

La surveillance prédictive ne vise plus seulement à savoir ce que le travailleur fait, mais à anticiper ce qu'il pourrait faire. Selon Schellmann (2024), ces outils promettent d'estimer le risque de départ d'un salarié, d'identifier des « hauts potentiels » susceptibles d'être promus, de repérer ceux qui réussiront le mieux dans un poste donné, mais aussi de signaler des « employés à problèmes », peu performants ou conflictuels. L'offre s'est surtout développée aux États-Unis, où prospère une industrie de l'analyse des données

¹⁶ Règlement européen 2024/1689 du 13 juin 2024 sur l'intelligence artificielle, article 5. Point f.

¹⁷ Sur ces programmes et leurs implications, voir Ajunwa (2023), chap. 7, qui en fait l'un des instruments de la quantification du travailleur.

de personnel, les « people analytics » ; sa diffusion en Europe reste limitée. Ces outils reposent sur une mise en données du travail et des travailleurs. Ils exploitent d’abord les données que l’entreprise possède déjà (ancienneté, évaluations, promotions, salaire, absentéisme, enquêtes internes), auxquelles s'ajoutent les traces de l'activité quotidienne : volume de courriels, participation aux réunions, rythme de réponse aux messages, voire données extérieures comme l'activité sur LinkedIn. Ces données sont ensuite traitées par apprentissage supervisé, selon le principe présenté précédemment. Pour prédire les démissions, par exemple, le modèle est entraîné sur les dossiers des salariés partis au cours des années précédentes et sur ceux des salariés restés : il y repère les régularités qui distinguent les uns des autres, telles qu'une ancienneté dans le poste sans promotion, une baisse de participation aux réunions ou un ralentissement des réponses aux messages. Appliquées aux salariés actuels, ces régularités produisent un score de risque de départ. Le modèle ne comprend pas pourquoi un salarié part : il constate que certains profils ressemblent à ceux qui sont partis.

Mais ces outils posent plusieurs problèmes. Le premier est leur manque de fiabilité. Hilke Schellmann les a testés. Ses tests portent sur des dispositifs d'évaluation de candidats à l'embauche, mais les techniques sont celles-là mêmes de la prédiction interne. Son expérience la plus parlante concerne un logiciel d'entretien vidéo automatisé, auquel elle répond intégralement en allemand, en lisant une page Wikipédia sur la psychométrie, alors que l'entretien est censé évaluer son adéquation à un poste en anglais. Le logiciel ne signale aucune anomalie : il lui attribue 73 % d'adéquation, et une étudiante qui refait l'expérience en chinois obtient même 80 %. L'explication du fournisseur est plus révélatrice encore que l'échec du test : le score reposerait surtout sur l'intonation, le ton et la hauteur de la voix, plutôt que sur le contenu des réponses. Ce qu'ils mesurent n'est pas ce qu'ils prétendent prédire. Ce manque de fiabilité tient aussi à ce que ces outils ignorent le contexte. Un salarié peut partir pour des raisons que l'entreprise ne mesure pas ou mal : opportunité d'emploi extérieure, situation familiale, état du marché du travail, aspirations personnelles. Cette cécité conduit à des contresens. Un manager pourra ainsi être identifié comme problématique parce que son service connaît de nombreux départs, alors que ces départs traduisent peut-être l'inverse : un manager qui forme ses collaborateurs et favorise leur mobilité vers d'autres services.

Les biais constituent un deuxième problème. Les promoteurs de ces outils vantent parfois leur objectivité : là où le jugement humain reste exposé aux préjugés, l'algorithme traiterait chacun de la même manière. L'exemple, devenu classique, d'Amazon montre ce qu'il en est. L'entreprise avait entraîné un algorithme de recrutement sur dix ans de candidatures, majoritairement masculines ; le modèle a appris à privilégier les CV d'hommes et à pénaliser certains termes associés aux femmes. Il ne repérait donc pas les meilleurs candidats : il reproduisait les régularités d'un passé déjà inégalitaire. Amazon a abandonné ce projet en 2018, mais la pratique s'est généralisée, les entreprises recevant trop de candidatures pour les lire humainement, et l'enquête de Schellmann montre que des critères en apparence neutres y fonctionnent comme des indicateurs indirects de genre, d'origine ou de handicap. Le même mécanisme vaut au-delà du recrutement : si les données passées reflètent des inégalités d'accès aux promotions ou aux évaluations positives, un modèle chargé d'identifier les « hauts potentiels » favorisera les profils qui ressemblent aux salariés historiquement valorisés. Les biais ne disparaissent donc pas avec l'automatisation ; ils deviennent moins visibles et plus difficiles à contester.

Troisième problème, le risque de prophétie auto-réalisatrice. Une fois qu'un salarié est

identifié comme présentant un risque de départ, cette information peut modifier le regard porté sur lui. Le manager peut être tenté d'anticiper son départ en limitant les investissements jugés trop coûteux ou trop incertains : promotion, formation, augmentation, nouvelles responsabilités. La prédiction devient alors performative : en traitant le salarié comme quelqu'un qui va partir, l'organisation contribue à produire le départ qu'elle croyait seulement prévoir.

Au terme de cette section, une figure se dessine : celle du « travailleur quantifié » décrite par Ajunwa (2023). Elle désigne toutefois un possible, non un état accompli : restent à examiner leurs effets sur les travailleurs, leur diffusion réelle et les mécanismes qui en modulent le déploiement.

Les effets de la surveillance sur les conditions de travail

Ces capacités nouvelles ne produisent pas partout ni toujours les mêmes effets. Lorsqu'elles s'inscrivent dans un management qui prescrit et évalue individuellement le travail, elles agissent selon trois registres liés : elles *réduisent les marges d'autonomie*, *intensifient le travail* et, par leur combinaison, *affectent la santé des travailleurs*.

Perte d'autonomie

La surveillance numérique peut réduire fortement l'autonomie des travailleurs, en particulier lorsqu'elle s'inscrit dans des formes de management algorithmique, où le logiciel ne se contente pas d'observer mais prescrit lui-même les tâches et en contrôle l'exécution. Surveillance et prescription sont alors indissociables : c'est parce que l'activité est intégralement tracée que la prescription peut se faire en temps réel, geste après geste. On retrouve, automatisé, le couple taylorien déjà décrit : connaître le travail pour mieux le prescrire. Dans les entrepôts évoqués, le logiciel retire ainsi au préparateur une part des choix qui constituaient son savoir-faire : parcours, ordre des prélèvements, organisation de la palette sont désormais déterminés par le système.

Cette perte d'autonomie s'accompagne d'une déqualification : Gautié et Perez (2023) notent que le temps nécessaire pour rendre un nouvel opérateur autonome est passé de deux ou trois semaines à deux ou trois jours. Le témoignage d'un préparateur sous commande vocale en livre une image éloquente : se sentant « transformé en robot », il résume sa journée d'un « on est branché quand on commence, on est débranché à la fin ». Réduit à un « appendice de la machine »¹⁸, le travailleur devient le bras prolongé du flux numérique dans l'espace physique. Les entrepôts ne constituent pas un cas isolé. Les techniciens de maintenance itinérants (voir supra) disposaient d'une autonomie professionnelle réelle : responsables de certains sites, ils connaissaient leurs installations et estimaient eux-mêmes le temps nécessaire à une intervention. L'application leur indique désormais le client à visiter, l'ordre des opérations, les tâches à effectuer et la durée prévue, au point qu'ils parlent d'une « rigidité numérique » qui rend difficile de s'écarter de la procédure pour tenir compte de la situation concrète. Leur expertise s'est en partie déplacée vers le système, qui estime à leur place ce qu'ils savaient évaluer. La logique est la même que dans l'entrepôt : plus l'activité est finement observée, plus elle peut être prescrite dans le détail, et moins il reste d'espace pour le jugement du travailleur.

Intensification du travail

La surveillance numérique contribue à l'intensification du travail, c'est-à-dire au fait de produire davantage par unité de temps. Elle emprunte deux voies : les algorithmes organisent un travail plus dense et la mesure permanente de l'activité incite les travailleurs

¹⁸ L'expression de Karl Marx est reprise par Gautié et Perez (2023)

à accélérer leur rythme. L'intensification passe d'abord par la rationalisation de l'organisation du travail, dans le prolongement du bureau des méthodes taylorien. Les logiciels d'optimisation prescrivent les parcours de collecte dans les entrepôts, découpent les tournées des livreurs, recalculent les itinéraires en temps réel et compressent les durées allouées à chaque tâche. Moins de temps morts, un rythme plus élevé : soit davantage d'articles collectés, de colis livrés, de clients servis dans la même journée. La cadence est incorporée dans la prescription, et l'intensification se confond avec la perte d'autonomie décrite précédemment : c'est parce que l'algorithme dicte le parcours et l'ordre des tâches qu'il peut en éliminer tout le mou.

Les dispositifs numériques ne se contentent cependant pas d'organiser un travail plus dense : ils mesurent l'activité et font de cette mesure un aiguillon. Cette pression s'exerce en premier lieu par la chasse aux temps morts, ainsi du logiciel de télétravail, qui décomptait toute période sans frappe ni mouvement de souris. C'est la « flânerie » que combattait déjà Taylor, désormais traquée sans interruption ni surveillant. La mesure élève ensuite les cadences du travail effectif lui-même, par la conversion de l'activité en indicateurs de productivité : vitesse de scannage, nombre d'articles prélevés par heure, nombre d'appels traités, temps par intervention rapporté à la durée cible. Dès qu'un paramètre est mesuré, il devient un objectif à atteindre, puis à dépasser ; chaque écart doit être justifié. Le logiciel de gestion des interventions de Microsoft (Dynamics 365 Field Service), utilisé pour piloter le travail des techniciens de maintenance itinérants, affiche ainsi en continu sur le *smartphone* du salarié l'écart entre la durée prévue et la durée réelle de l'intervention, et peut l'avertir lorsqu'il approche du plafond de coût associé à l'ordre de travail (Christl, 2024). Les mêmes logiciels comparent et hiérarchisent les techniciens, en affichant par exemple un « top 5 » rapporté aux moyennes de l'équipe : s'installe une émulation permanente qui tire les cadences vers le haut sans consigne explicite d'accélération, d'autant plus efficace que la rémunération est parfois indexée sur ces scores.

Le contrôle finit par se déplacer vers le travailleur lui-même. Dans la *start-up* parisienne dont il a été question, l'équipe de développeurs reçoit chaque matin un récapitulatif des tâches en cours, à charge pour chacun d'expliquer ses retards ; toutes les deux semaines, les salariés doivent analyser leur propre productivité et proposer des pistes d'amélioration : le travailleur devient son propre contrôleur de gestion. Dans ces configurations, l'indicateur ne se contente donc pas d'enregistrer l'intensité du travail : il contribue à la produire, en substituant au contremaître une discipline chiffrée et continue, d'autant plus difficile à contester qu'elle se présente comme une description objective de l'activité.

L'intensification n'est pourtant pas une conséquence automatique de la numérisation. Dans les hôpitaux français et italiens étudiés par Rani, Pesole et González Vázquez (2024), les outils numériques améliorent la coordination et réduisent certaines tâches non médicales. Dans les services d'urgence français, des dispositifs prédictifs permettent en outre d'anticiper les flux de patients et d'ajuster les ressources. À horaires inchangés, les soignants interrogés font état d'une charge de travail mieux organisée, d'une pression moindre et de moins de stress ; aucun des salariés interrogés dans les deux cas français ne rapporte d'intensification du travail. Dans le cas sud-africain étudié par les mêmes auteurs, le suivi numérique des performances s'accompagne au contraire d'une intensification du travail de certains professionnels. Le numérique peut ainsi desserrer la contrainte temporelle lorsqu'il sert à anticiper les flux et à répartir les ressources, ou la renforcer lorsqu'il est utilisé pour relever les objectifs, comparer les performances individuelles et

supprimer les temps improductifs. Ses effets dépendent moins de ses seules capacités techniques que des usages managériaux et du cadre organisationnel dans lesquels il s'inscrit.

Des effets sur la santé des travailleurs

L'intensification produite par les dispositifs numériques de surveillance ne reste pas sans conséquences sur la santé des travailleurs. Les atteintes sont d'abord physiques. Une charge de travail élevée et des rythmes rapides sont associés à des risques accrus de troubles musculo-squelettiques et d'accidents du travail (Boini et al., 2024). Dans les entrepôts, les gestes répétitifs et le port de charges lourdes peuvent ainsi provoquer des lésions nerveuses et musculaires chroniques, d'autant plus fréquentes que l'optimisation des cadences supprime les micro-pauses par lesquelles le corps amortissait la répétition des efforts (Benvegnù et Gaborieau, 2020). Les effets sont également psychiques. La revue de littérature réunie par Molnar (2025) montre que les salariés soumis à une surveillance électronique déclarent davantage de tension, d'anxiété, de fatigue et de symptômes dépressifs que les salariés non surveillés. D'autres études associent le contrôle électronique à l'épuisement émotionnel et au *burn-out*. La surveillance agit directement, par le sentiment d'être constamment observé, mais aussi indirectement, en accroissant la charge, en raréfiant les temps de relâchement et en alimentant l'incertitude sur l'avenir professionnel. Le salarié mesuré en continu peut alors avoir le sentiment d'être toujours en retard, toujours évalué, toujours comparé : l'impossibilité d'échapper au regard de l'organisation nourrit une anxiété et une insécurité durables.

Dans les activités de service s'ajoute une contrainte d'un autre ordre : le contrôle porte également sur les émotions. Face au client, il faut sourire, contenir son irritation, ce que la sociologie désigne comme le travail émotionnel¹⁹. Les évaluations par les clients transforment cette exigence diffuse en performance quantifiée : notes et commentaires incitent le salarié à discipliner en permanence son comportement et l'expression de ses émotions. Or la nécessité de maîtriser continuellement ses émotions est associée au syndrome d'épuisement professionnel, notamment à l'épuisement émotionnel, ainsi qu'à des risques accrus d'anxiété et de troubles dépressifs (Boini et al., 2024). Ces effets ne sont pourtant pas mécaniques. Certains dispositifs de suivi sont installés au nom de la santé et de la sécurité : ils peuvent détecter la fatigue d'un conducteur, signaler une chute ou déclencher une alerte en cas d'accident. L'enregistrement des données peut également protéger le travailleur contre l'arbitraire en fournissant une preuve objective. Les chauffeurs routiers américains étudiés par **Karen Levy** (2023) doivent ainsi être équipés, depuis 2017, d'un enregistreur automatique de leurs heures de conduite. Certains se sont approprié cet outil pour refuser une course supplémentaire : l'appareil atteste que la durée légale de conduite est épuisée et leur permet d'opposer la règle aux exigences de l'employeur. La donnée qui surveille est aussi celle qui protège. Le même exemple révèle toutefois les limites de cette protection. La fatigue des chauffeurs tient moins au seul dépassement des durées légales qu'à un modèle économique fondé sur le paiement au kilomètre et sur des temps d'attente non rémunérés, que l'enregistreur laisse intacts. Le décompte automatique rend même les horaires plus rigides : pour ne pas perdre le temps de conduite encore disponible, certains chauffeurs peuvent être conduits à rouler dans de mauvaises conditions ou à accélérer. Les infractions diminuent, sans que la baisse des accidents soit avérée. La mesure protège ainsi contre certains abus, mais elle ne corrige pas les causes économiques et organisationnelles des conduites à risque.

Plus largement, les effets de la surveillance dépendent de la manière dont elle est conçue et mise en œuvre (Molnar, 2025). Lorsqu'elle est transparente, perçue comme équitable et que

¹⁹ Concept forgé par A. R. Hochschild (1983)

les salariés participent à sa définition, ses effets négatifs sur la santé peuvent être atténués. Un suivi destiné à fournir un retour constructif peut même améliorer la satisfaction au travail, tandis que des indicateurs portant sur les performances collectives plutôt qu'individuelles peuvent favoriser une meilleure répartition des efforts et davantage de coopération. Ces résultats nuancent le constat sans l'inverser : les auteurs concluent à une prédominance des effets négatifs, notamment sur le bien-être. Perte d'autonomie, intensification, atteintes à la santé : le tableau reste sombre. Il faut maintenant l'éprouver. Ce que l'on vient de décrire est-il l'expérience ordinaire du travail salarié, ou l'exception que produisent quelques secteurs ?

Quelle est l'ampleur de la surveillance numérique ?

Deux enquêtes publiées en 2025 abordent le phénomène par deux versants complémentaires. L'enquête de l'OCDE interroge plus de 6 000 cadres dirigeants dans six pays, dont la France et les États-Unis (Milanez et al., 2025). L'enquête AIM-WORK du Centre commun de recherche de la Commission européenne interroge quant à elle plus de 70 000 travailleurs des vingt-sept États membres (Gonzalez Vazquez et al., 2025). Du côté des salariés européens, l'enquête AIM-WORK montre que la surveillance numérique est déjà courante, mais qu'elle reste principalement centrée sur le temps et la présence. Les formes les plus fréquentes sont le suivi du temps de travail, qui concerne 37 % des travailleurs, et le contrôle des entrées, sorties et déplacements par badges, 36 %. Les autres formes sont nettement moins répandues : vidéosurveillance et suivi de l'usage d'internet, 14 % chacun, surveillance des appels et *e-mails*, 12 %, usage de l'ordinateur, 11 %, localisation dans les véhicules, 9 %, réseaux sociaux, 7 %.

Du côté des entreprises, l'enquête de l'OCDE révèle une diffusion beaucoup plus massive aux États-Unis, où 90 % des entreprises utilisent au moins un dispositif de surveillance, contre 67 % en Europe. Le suivi du temps de travail y concerne 88 % des entreprises contre 44 % en Europe, celui des tâches réalisées 86 % contre 40 %, celui de la vitesse d'exécution 72 % contre 15 %. L'écart devient plus net encore pour les formes les plus profondes : la surveillance du contenu et du ton des conversations concerne 55 % des entreprises américaines, contre 6 % des européennes.

Ces deux enquêtes donnent un état des lieux, non une évolution. Les enquêtes (2017) de la Direction de l'animation de la recherche, des études et des statistiques (DARES) sur les conditions de travail permettent seules, pour la France, de suivre une évolution. Elles montrent une augmentation importante des contraintes de rythme liées à des dispositifs numériques. En 2016, 35 % des salariés du privé déclaraient que leur rythme de travail était imposé par un contrôle ou un suivi informatisé, contre 25 % en 2005.

Ces données dessinent une diffusion réelle mais concentrée, centrée sur le temps, la présence et les déplacements, et nettement plus poussée aux États-Unis qu'en Europe. Les formes les plus intrusives, celles qui touchent aux communications ou aux comportements, restent en Europe le fait d'une minorité d'entreprises et de secteurs. La question posée en introduction reçoit là un début de réponse : les organisations ne font pas tout ce que la technique permet. Reste à comprendre ce qui freine ou module ce déploiement.

Les filtres de la surveillance

Une extension continue des capacités de surveillance a été décrite, au point de laisser croire à un mouvement inéluctable. Le potentiel est, de fait, considérable : la plupart des travailleurs utilisent désormais des dispositifs numériques qui enregistrent leur activité.

Les enseignants eux-mêmes n'y échappent pas : leur environnement numérique de travail permettrait de compter les connexions, le nombre de devoirs, les délais de correction des copies ou de réponse aux parents. Mais l'expérience commune est là : cette surveillance possible ne s'exerce guère. Leur usage n'est pas davantage univoque : les mêmes indicateurs peuvent alimenter un contrôle individualisé ou soutenir la coordination et l'apprentissage collectif. Le numérique fournit donc une infrastructure sans en déterminer ni l'activation ni la finalité. Le constat rejoint celui des premiers propos : il n'a pas créé le projet de surveiller le travail, déjà présent chez Taylor, mais en a levé les contraintes techniques. Restent les filtres sociaux – le droit, les pratiques des managers et les contre-pouvoirs collectifs – qui en limitent le déploiement et en orientent les usages.

Filtre	Comment limite-t-il la surveillance ou en oriente-t-il les usages ?
Le droit	Il encadre la collecte et l'utilisation des données des travailleurs - Le RGPD impose notamment une finalité légitime et un traitement proportionné - L'AI Act interdit certains usages et soumet les systèmes à haut risque à des obligations renforcées.
Le management	Il détermine l'usage effectif des données - Il sélectionne les indicateurs, leurs destinataires et les usages qui en sont faits. - Il peut utiliser les données pour prescrire, comparer et sanctionner, ou les mettre au service de l'autonomie, du retour d'expérience et de l'apprentissage collectif. - Les normes valorisant la confiance et la responsabilisation rendent plus difficile la légitimation d'un contrôle permanent.
Les contre-pouvoirs collectifs	Ils permettent aux travailleurs de peser collectivement sur le déploiement des dispositifs et l'usage des données. - Les représentants peuvent rendre les dispositifs visibles, en négocier les usages et les évolutions, ou les contester. - Leur participation à la définition et à l'interprétation des indicateurs donne aux travailleurs davantage de prise sur l'usage des données. - Les travailleurs peuvent mobiliser leur place dans la production et leur capacité d'action collective.

Ces filtres sont partiels, et c'est en observant où ils cèdent qu'on mesure leur portée exacte. Ils n'en sont pas moins réels, et le contraste transatlantique suffira à le montrer. Le droit encadre davantage qu'il n'interdit : il limite le pouvoir de contrôle de l'employeur sans le remettre en cause. L'information des salariés ne leur confère aucun pouvoir de décision : être informé ne signifie pas pouvoir refuser un outil ni en bloquer le déploiement. Et l'application du RGPD repose sur des notions souples, intérêt légitime, nécessité, proportionnalité, dont l'interprétation ménage aux entreprises une marge considérable, que leurs conseils n'ont pas manqué de repérer : Zuboff (2020) cite un livre blanc présentant l'intérêt légitime comme une occasion de contourner les nouveaux obstacles réglementaires. Le contentieux Amazon France Logistique montre que cette marge joue aussi devant le juge. Là où la CNIL avait jugé excessifs plusieurs indicateurs de suivi de l'activité, dont la mesure des temps d'inactivité et de la latence entre deux scans, le Conseil d'État a validé ces traitements, les estimant justifiés par les contraintes propres à l'activité logistique. Un suivi très fin devient ainsi licite dès lors qu'il se rattache à une finalité professionnelle reconnue. L'AI Act souffre d'une fragilité d'une autre nature, puisque l'évaluation de conformité des systèmes à haut risque incombe pour l'essentiel au fournisseur lui-même : les producteurs d'outils de surveillance certifient leurs propres produits et la protection dépend de la qualité de cette autoévaluation comme de la capacité des autorités à contrôler ensuite les pratiques. La modération managériale,

ensuite, est ambivalente. L'étude de cas menée par **Grégory Jemine** (2019) dans une compagnie d'assurances belge montre des managers de proximité qui relativisent la fiabilité des indicateurs et refusent d'y réduire l'évaluation de leurs collaborateurs. Mais cette retenue protège d'abord leur propre position : reconnaître aux chiffres le pouvoir de dire la valeur d'un salarié reviendrait à céder au système ce qui fonde leur légitimité, le jugement sur les hommes. Elle protège aussi les ressources de leur service : aucun manager ne cherche à ramener à zéro le stock de dossiers en attente, une telle situation risquant de révéler un surplus d'effectifs. S'y ajoute une contradiction plus large, entre des outils de *monitoring* d'inspiration taylorienne et des discours managériaux qui promeuvent la confiance et l'autonomie : dès lors qu'ils adhèrent au second, les managers peinent à légitimer le premier. Le filtre tient donc à des intérêts et à des normes, non à un principe : il peut disparaître si les uns ou les autres changent.

Cette ambivalence apparaît plus nettement encore dans la comparaison menée par Ahlstrand et Gautié (2018). Dans les établissements aéronautiques français étudiés, les indicateurs associés au *Lean*²⁰ alimentent d'abord le reporting et le contrôle hiérarchique, au point qu'un directeur de division déclare en suivre environ deux cents et que les managers de proximité consacrent davantage de temps à les vérifier et moins de temps à discuter avec les salariés dans les ateliers. Dans les établissements suédois, où les auteurs n'observent pas la même inflation du *reporting*, les indicateurs sont davantage intégrés au fonctionnement d'équipes autonomes et à la résolution collective des problèmes. Ce contraste ne tient cependant pas seulement aux dispositifs. Dans les établissements français, les réunions quotidiennes autour des indicateurs de sécurité, de qualité, de coûts, de délais et de personnel se réduisent souvent à une vérification de listes et à une transmission descendante d'informations. Mais, dans une division ayant expérimenté une organisation plus autonome, elles sont désormais animées par les opérateurs, qui peuvent tester directement des améliorations du processus. Les indicateurs changent alors de fonction : imposés d'en haut, ils servent le contrôle ; discutés et appropriés par les équipes, ils peuvent soutenir la coordination, l'autonomie et l'apprentissage collectif.

Cette appropriation des indicateurs ne dépend toutefois pas du seul management : elle suppose que les travailleurs et leurs représentants disposent des moyens d'intervenir sur la conception et l'usage des dispositifs. Or ces contre-pouvoirs collectifs restent fragiles. En Autriche, les comités d'entreprise disposent d'un droit de codétermination lors de l'introduction des systèmes de contrôle. Dans une entreprise étudiée par Christl (2024), le comité a ainsi négocié l'usage de l'application de suivi des techniciens de maintenance. Mais l'accord ne couvre pas le progiciel qui pilote cette application, lequel peut ensuite être mis à jour sans nouvelle consultation. Le dispositif évolue plus vite que la négociation.

Le pouvoir de blocage, lui, est paradoxalement fort là où la surveillance est la plus intense : dans une logistique en flux tendu, sans stocks pour amortir l'interruption, une grève d'entrepôt se propage immédiatement à toute la chaîne. Encore faut-il pouvoir se mobiliser. Le conflit qui oppose depuis plus de dix ans le syndicat ver.di à Amazon en Allemagne l'illustre : les grèves y sont déclenchées lors des pics d'activité, mais l'entreprise, qui peut reporter l'activité sur ses autres entrepôts, n'a toujours pas signé la convention collective réclamée. Et la déqualification que la surveillance accompagne, en réduisant la formation à quelques jours, facilite le recours à une main-d'œuvre précaire et de passage, peu syndiquée et difficile à mobiliser. L'organisation du travail donne ainsi aux travailleurs un fort pouvoir de blocage mais les prive des moyens de l'exercer. Ces limites ne doivent pourtant pas faire conclure à l'inefficacité des filtres. Le contraste américain le montre a

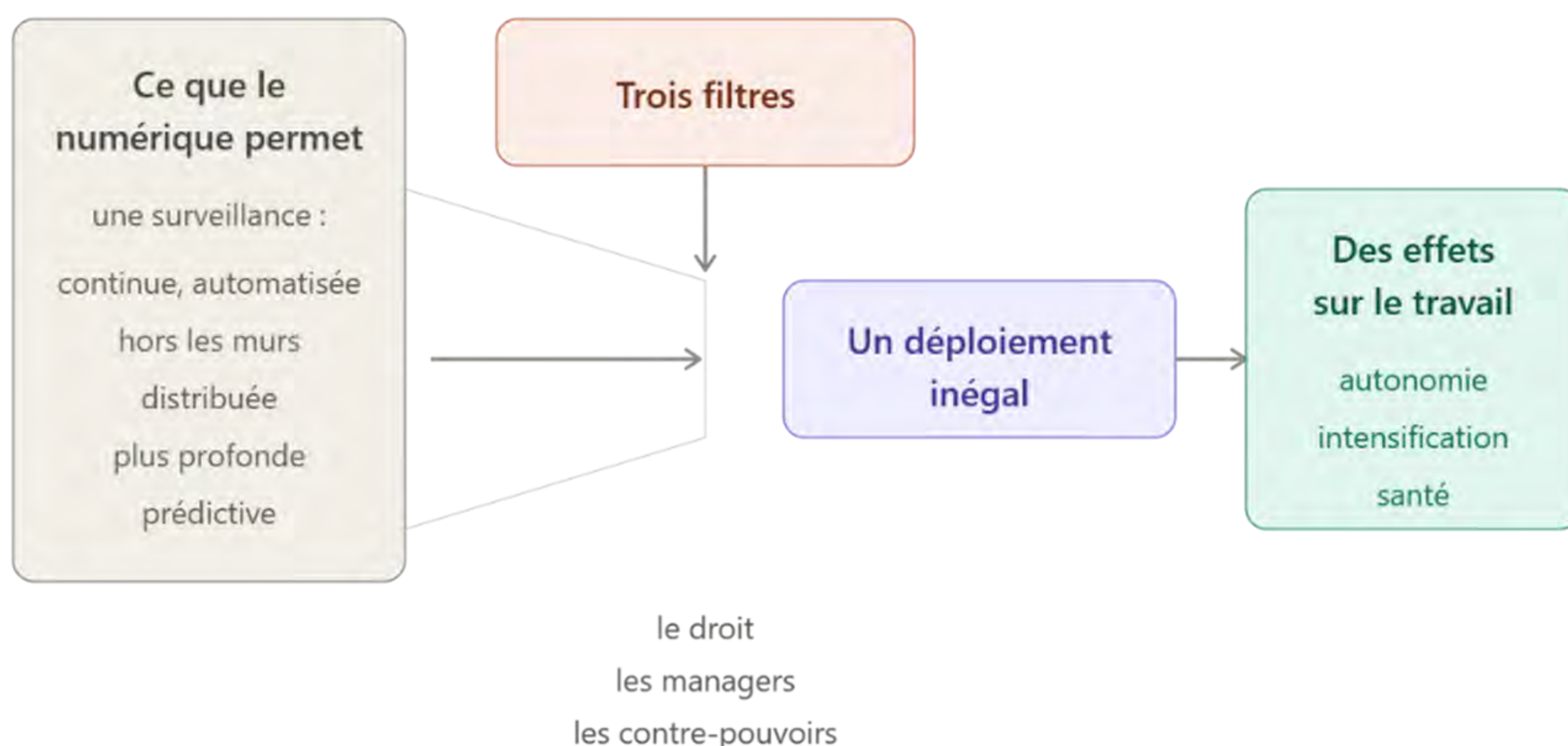
²⁰ Formalisé à partir du système de production de Toyota, le *Lean management* vise à éliminer tout ce qui ne crée pas de valeur dans le processus productif (stocks, attentes, déplacements, défauts) et à améliorer continuellement le processus. Il associe standardisation, suivi des performances et participation des salariés, selon des modalités variables.

contrario. Comme l'analyse Ifeoma Ajunwa (2023), trois traits y ont offert à la surveillance un terrain particulièrement favorable. La principale protection constitutionnelle contre les intrusions dans la vie privée, le Quatrième Amendement, ne pèse que sur les pouvoirs publics : elle ne s'impose pas aux employeurs privés, dont les salariés ne disposent d'aucun garde-fou fédéral équivalent. Les États-Unis n'ont pas de loi générale sur les données personnelles comparable au RGPD, mais un *patchwork* de dispositions sectorielles qui ne reconnaît presque aucun droit substantiel aux travailleurs. Enfin, la flexibilité de l'emploi, qui autorise un licenciement quasi discrétionnaire, prive le salarié de toute possibilité réelle de refuser un dispositif sans risquer son poste. Le résultat se lit dans les chiffres : à technologies identiques, 90 % des entreprises américaines utilisent au moins un dispositif de surveillance contre 67 % des européennes, et la surveillance des conversations concerne 55 % des premières contre 6 % des secondes. L'écart ne s'explique pas par la technique : il mesure ce que pèsent les protections.

Ces filtres ne sont ni indépendants ni absolus. Le droit ne devient effectif que si des acteurs s'en saisissent ; les représentants des salariés ne peuvent négocier que si le cadre institutionnel leur en donne les moyens ; les managers peuvent, selon leurs intérêts, limiter ou intensifier l'exploitation des données. La surveillance effectivement exercée dépend ainsi moins des capacités techniques que des rapports de force qui traversent les organisations et les sociétés.

Conclusion

La surveillance du travail n'est née ni avec Taylor ni avec le numérique : elle prend appui sur un pouvoir de contrôle inscrit dans la relation salariale elle-même. Taylor l'a érigé en programme méthodique d'organisation du travail, fondé sur la mise en visibilité de l'activité afin de la connaître, de la prescrire et de la contrôler. Le numérique en démultiplie aujourd'hui les possibilités en rendant la surveillance continue, mobile, distribuée et toujours plus profonde. Lorsqu'elles servent à prescrire et à évaluer individuellement le travail, ces capacités peuvent réduire l'autonomie, intensifier le travail et affecter la santé des travailleurs. Mais ces effets ne découlent pas mécaniquement des outils : les mêmes indicateurs peuvent alimenter un contrôle hiérarchique individualisé ou soutenir la coordination, l'autonomie et l'apprentissage collectif.



La question posée au départ reçoit donc une réponse négative : les organisations ne font pas tout ce que la technique permet. La surveillance la plus courante reste centrée sur le temps et la présence, tandis que les formes les plus intrusives demeurent minoritaires en

Europe et y sont bien moins diffusées qu'aux États-Unis. La technologie fournit l'infrastructure de la surveillance, mais elle n'en détermine ni l'ampleur ni les usages. Le droit, le management et les contre-pouvoirs collectifs ne décident pas seulement jusqu'où elle se déploie : ils orientent aussi la manière dont les données sont interprétées et mobilisées. La surveillance tend ainsi à se développer plus facilement là où les travailleurs disposent de peu de moyens pour la contester, et à être davantage contenue là où le droit, les représentants des salariés ou les managers lui opposent des limites. Elle ne dit donc pas seulement ce que la technique permet : elle révèle qui, dans chaque organisation et chaque société, dispose du pouvoir de définir le travail.

La plainte de l'ouvrier de 1911, qui ne pouvait plus « penser ou bouger » sans qu'on lui dise comment faire, trouve ainsi un écho chez le préparateur guidé à la voix ou le technicien minuté par son application. Un siècle plus tard, la même question se pose avec une acuité renouvelée : jusqu'où contrôler le travail sans faire disparaître ce qui en fait une activité humaine, faite de jugement, d'initiative et de coopération ?



Source gallica.bnf.fr / Bibliothèque nationale de France

Une de la revue trimestrielle *Prosperité* (avril 1931) documentant l'introduction d'un outil de mesure du temps destiné à rationaliser et optimiser l'organisation scientifique du travail (OST). [Gallica](https://gallica.bnf.fr/)

La surveillance des infrastructures de l'information : état de la menace

Dans les infrastructures informatiques, la surveillance est étroitement liée à la menace cyber. Ce développement invite à s'immerger dans la fonction d'un responsable de site informatique faisant face à une cyberattaque de son réseau.

Si l'on souhaite avoir une bonne connaissance des dangers liés à la cybermenace, le [Panorama de la cybermenace 2025](#) publié par l'**ANSSI** dresse un état des tendances observées annuellement. L'analyse des incidents traités met en évidence des risques structurels affectant les infrastructures numériques françaises. Leur fréquence et leur gravité confirment la nécessité d'une « surveillance continue des systèmes d'information ». En 2025, la menace cyber confirmée comme durable et en progression reste à un niveau toujours élevé. L'ANSSI a traité 3 586 événements de sécurité. Même si l'on constate une diminution de 18 % par rapport à 2024 où le contexte des JO 2024 a créé un pic de signalements, la cybermenace conserve son caractère systémique. La menace touche l'ensemble du territoire, proportionnellement à l'activité économique.

Parmi les risques, les attaques à but lucratif demeurent centrales. Fondées sur l'extorsion (vol de données, chiffrement ou double extorsion), elles sont principalement menées par des groupes de [rançongiciel](#) dont l'activité reste élevée. Les pays économiquement développés sont particulièrement ciblés afin de maximiser les paiements. Les incidences sont significatives : indisponibilité prolongée des services, atteinte à la réputation et pertes financières. L'attaque en 2024 contre l'université Paris-Saclay, ayant perturbé des applications critiques en période d'inscription, illustre la gravité opérationnelle de ces incidents et souligne la nécessité de plans de continuité et de reprise d'activité. Ces attaques représentent ainsi un risque à la fois fréquent et fortement impactant.



Panorama de la cybermenace. ANSSI, 2025.
Open Licence (Étalab — V2.0). p.50

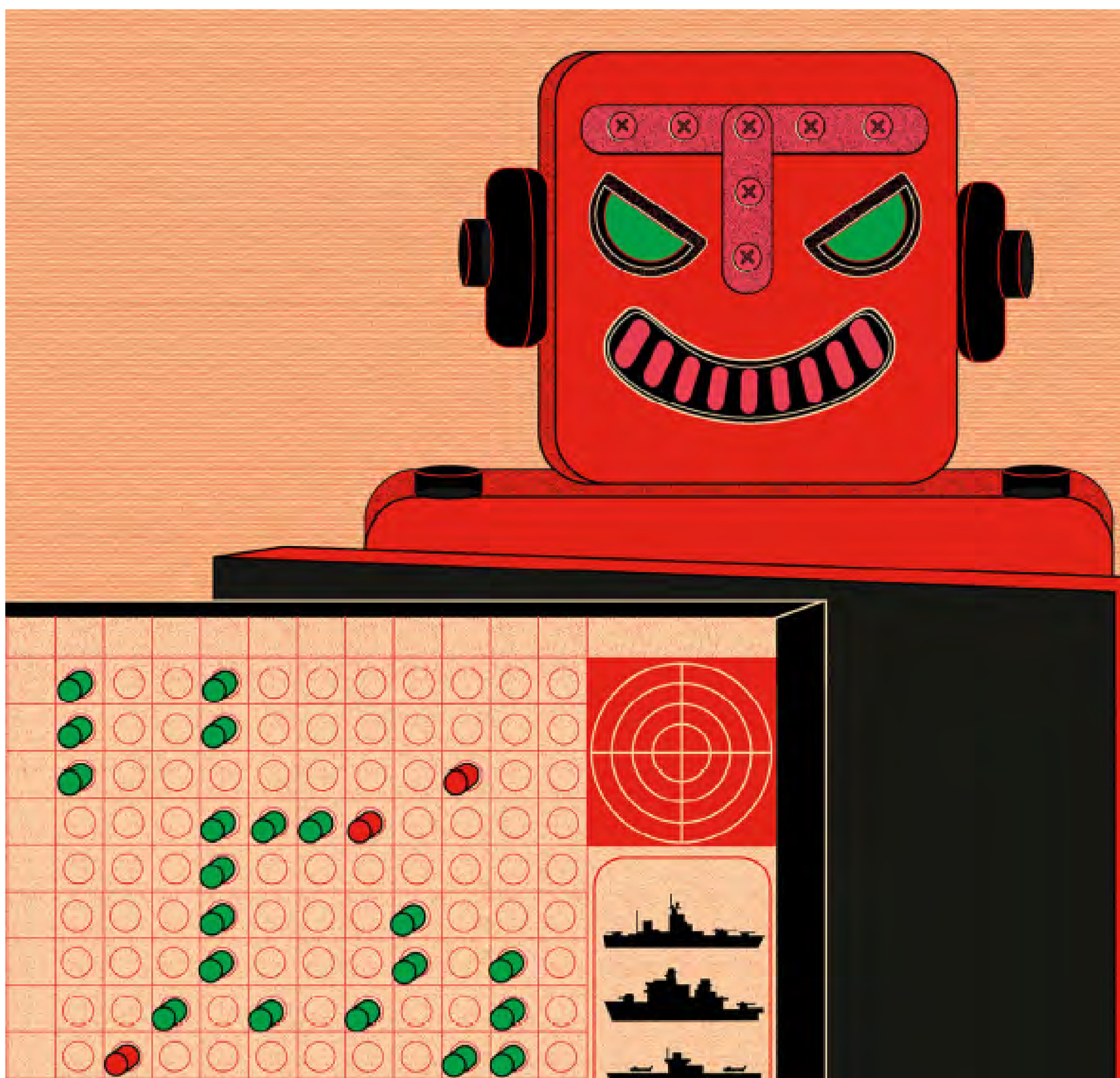
L'exploitation des vulnérabilités périmétriques : un risque hautement critique

Une majorité des opérations de cyberdéfense menées par l'ANSSI en 2025 ont pour origine l'exploitation de vulnérabilités affectant des équipements situés en bordure des systèmes d'information. Sont particulièrement concernés : les passerelles VPN, les équipements de sécurité réseau, les *appliances* exposées sur Internet. Ces équipements peuvent être insuffisamment sécurisés, mal configurés, ou dépourvus de capacités d'audit adaptées.

Plusieurs vulnérabilités critiques ont été exploitées en 2025 comme les années précédentes sur des équipements Ivanti, Palo Alto Networks, Fortinet ou Check Point, y compris des [vulnérabilités jour-zéro](#) (*zero-day*). Ces failles permettent l'exécution de code arbitraire à distance, le contournement des mécanismes d'authentification, ou l'accès à des ressources restreintes. L'exploitation de ces points d'entrée stratégiques peut conduire à une compromission globale du système d'information. Ce risque est hautement critique, car il concerne l'architecture même des infrastructures.

Les attaques de déstabilisation : impact opérationnel et symbolique

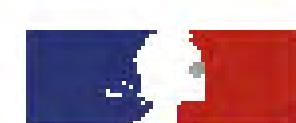
Une hausse des attaques en 2024, à finalité de déstabilisation a été constatée, notamment menées par des groupes *hacktivistes*. Des petites installations industrielles, particulièrement dans les secteurs de l'énergie renouvelable et de l'assainissement de l'eau, ont été ciblées via des interfaces de gestion exposées sur Internet. Dans un cas, un [parc éolien a été temporairement arrêté](#). Le panorama mentionne également des tentatives de sabotage de systèmes de contrôle industriel (ICS) dans le contexte du conflit en Ukraine. Ces attaques sont moins massives en volume, mais leur impact peut être opérationnel (interruption d'activité), symbolique (atteinte à la confiance) ou stratégique (pression politique), les infrastructures industrielles connectées devenant des cibles vulnérables.



Panorama de la cybermenace. ANSSI, 2025. Open Licence (Etalab — V2.0). p.23

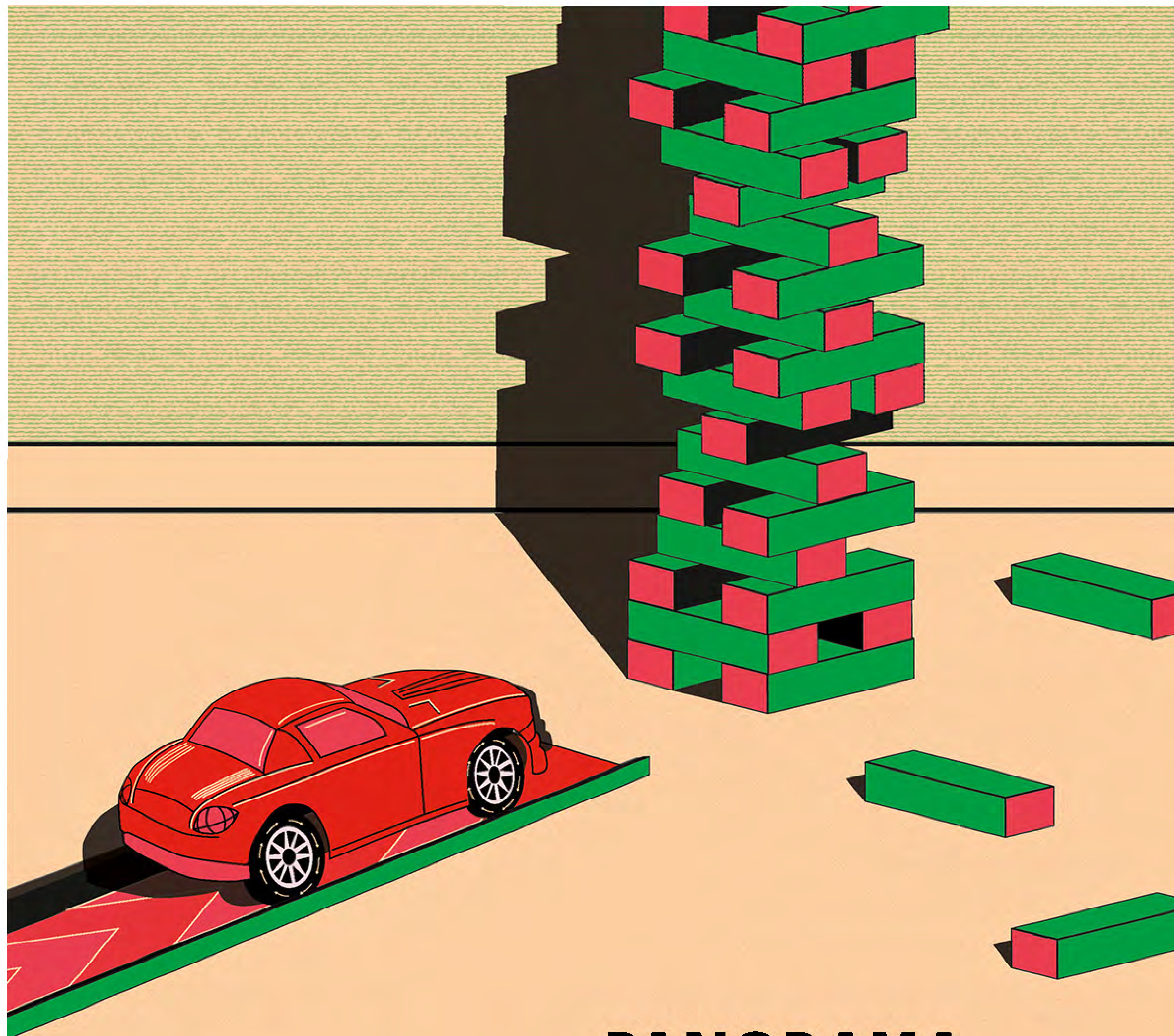
Les attaques d'espionnage : menace stratégique et persistante

Les attaques à finalité d'espionnage se distinguent par des compromissions étendues, une inscription dans la durée et des objectifs stratégiques. Les entités gouvernementales, diplomatiques, de recherche et les infrastructures essentielles constituent des cibles récurrentes. Ces attaques mobilisent fortement les équipes opérationnelles de l'ANSSI et nécessitent des investigations approfondies, des opérations de remédiation complexes et des efforts prolongés. L'étude mentionne notamment le ciblage des infrastructures de télécommunications. Ce risque est moins visible, mais systémique, visant la captation d'informations sensibles et l'affaiblissement à long terme des capacités nationales.



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



PANORAMA DE LA CYBERMENACE 2025

Panorama de la cybermenace. ANSSI, 2025. Open Licence (Etalab — V2.0)

Surveillance et durcissement : une réponse structurelle

L'ANSSI opère un service de supervision combinant détection réseau et système. En 2024, 162 signalements avaient été adressés aux institutions étatiques bénéficiaires. Cependant, les dispositifs de détection ne sont pleinement efficaces que si le système d'information a été préalablement sécurisé selon une logique de défense en profondeur. La sécurisation de l'annuaire d'authentification, notamment [Active Directory](#), est identifiée comme prioritaire, compte tenu de son rôle central dans la gestion des accès et des privilèges. La surveillance doit donc s'accompagner d'un durcissement des configurations, d'une segmentation réseau adaptée, d'une maîtrise des accès administrateurs et d'une capacité d'analyse corrélée des événements.

Une menace différenciée exigeant une supervision permanente

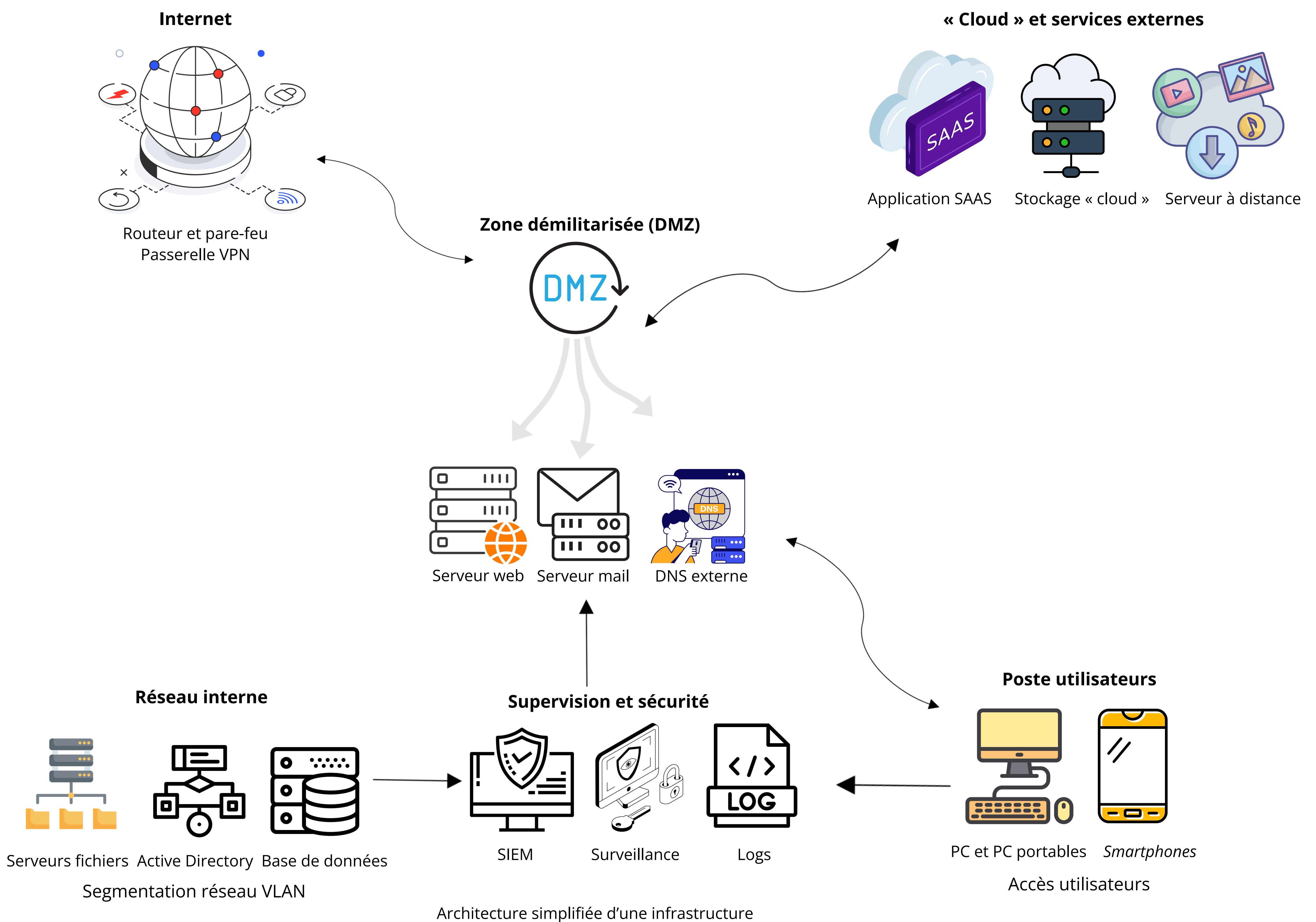
Les risques sont multiples : extorsion, sabotage, espionnage. Leur fréquence demeure élevée et leur dangerosité varie de l'indisponibilité ponctuelle à la compromission systémique. Dans ce contexte, la surveillance des infrastructures, fondée sur la journalisation, la supervision réseau et système, la corrélation des alertes et le durcissement préalable, constitue une réponse structurante face à une menace désormais installée dans la durée. Le déploiement d'outils de supervision active et d'une politique de journalisation rigoureuse devient ainsi une nécessité opérationnelle pour détecter et qualifier ces incidents au plus tôt.



Panorama de la cybermenace. ANSSI, 2025. Open Licence (Etalab — V2.0). p.42

L'organisation des systèmes informatiques : un cloisonnement indispensable

Une infrastructure informatique est organisée de manière hiérarchisée et segmentée afin d'assurer la performance, la sécurité, la disponibilité, la maîtrise des accès. Elle repose généralement sur une architecture en couches (schéma simplifié ci-après).



On distingue au sein de cet ensemble une infrastructure composée de plusieurs couches :

- La **couche périmétrique** (frontière avec Internet)

C'est la zone exposée où se positionnent le routeur d'accès Internet, le pare-feu (*firewall*), les concentrateurs [VPN](#), le *proxy*, le filtrage web. Son rôle est de contrôler les flux entrants et sortants, de bloquer les connexions non autorisées et d'isoler le réseau interne.

- La **DMZ** ([zone démilitarisée](#))

Dans cette zone intermédiaire entre Internet et le réseau interne, se trouvent le serveur web public, le serveur mail, le serveur DNS externe et le *reverse proxy*. Son rôle est d'héberger les services accessibles depuis l'extérieur et d'éviter un accès direct au réseau interne.

- Le **réseau interne** ([LAN](#))

C'est le cœur de l'organisation. Il est souvent segmenté en sous-réseaux ([VLAN](#) utilisateurs, VLAN serveurs, VLAN administration, VLAN Wi-Fi invité, VLAN imprimantes). Son rôle est de limiter la propagation d'une attaque et d'organiser les flux par métier. La défense se fait à ce stade en profondeur avec plusieurs niveaux de pare-feu pour davantage de sécurité.

- **Les serveurs et services centraux**

C'est le noyau stratégique du système d'information composé principalement d'un serveur d'authentification ([Active Directory](#)), de serveurs de fichiers, de serveurs applicatifs, de bases de données et [hyperviseurs](#) (virtualisation).

- **Les postes utilisateurs**

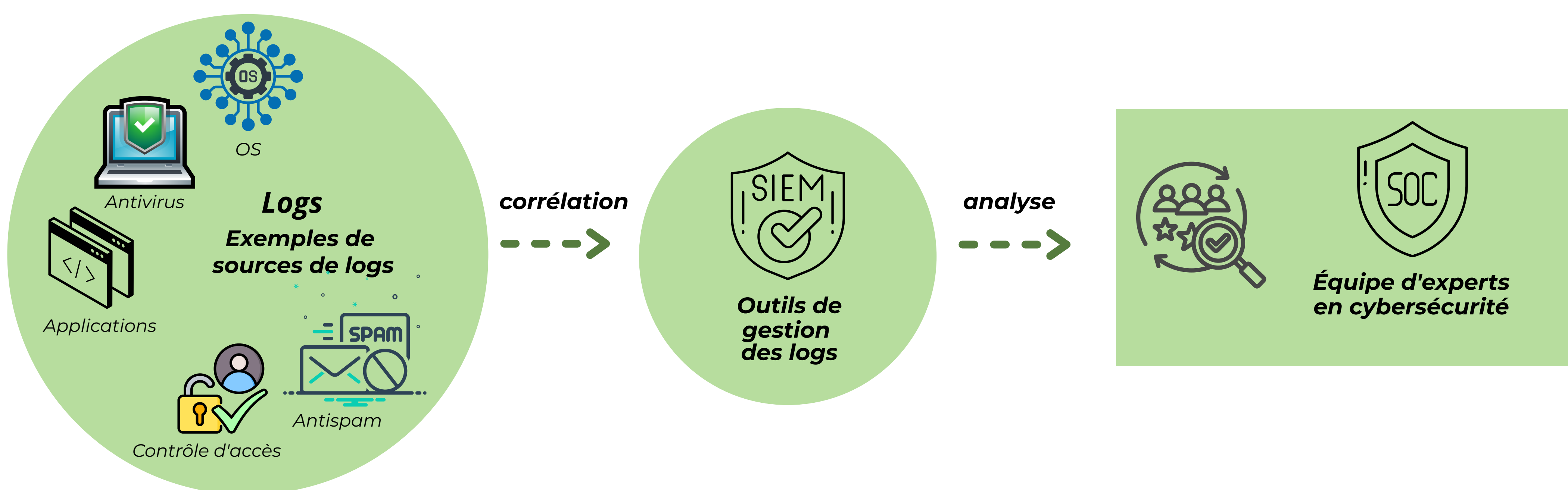
C'est souvent le point d'entrée principal des attaques par hameçonnage (*phishing*) et les logiciels malveillants. Leurs portes d'entrée sont les ordinateurs fixes, les PC portables et les [smartphones](#) professionnels. Le vecteur humain est très souvent la porte d'entrée d'une cyberattaque. L'ingénierie sociale (*social engineering*) est aussi un type d'attaque (usurpation d'identité, personnel de service externe, etc).

- **Le *cloud* et les services externes**

Aujourd'hui, les infrastructures sont hybrides. Ces éléments sont interconnectés avec le réseau interne via des tunnels sécurisés. Une organisation n'héberge plus tout localement dans sa salle serveur. Elle combine des ressources internes (serveurs, réseau, postes) que l'on appelle *on-premise* (sur site) et des ressources hébergées à distance dans des centres de données externes (*cloud*). C'est le cas des établissements scolaires où l'espace numérique de travail (ENT) se trouve à l'extérieur dans un *cloud*, géré par un fournisseur externe (souvent la région académique).

Une infrastructure moderne repose sur les fonctions suivantes : une segmentation réseau pour limiter les communications entre zones, un principe du moindre privilège pour que chaque utilisateur ou service ait uniquement les droits nécessaires, une *journalisation* systématique (les équipements peuvent être configurés pour produire des journaux d'événements ou *logs*), une supervision centralisée au sein d'un système [SIEM](#) (*security information and event management* ou gestion des informations et des événements de sécurité, supervision) et d'analyse des événements. Il est à noter que les *logs* ou journaux d'événements enregistrent automatiquement les actions et événements d'un système informatique (connexions, erreurs, accès à une donnée, etc), afin de surveiller l'activité et de détecter d'éventuels incidents.

Le SIEM permet de regrouper en un seul endroit l'exhaustivité de tous les *logs* du système d'informations. C'est le cœur de la cybersécurité. Un SIEM permet l'exploitation et l'analyse de centaines de milliers de *logs* simultanément, ce qui n'est pas possible manuellement par une personne.



Dans les environnements modernes, le [SOAR](#) (*security orchestration, automation and response*) se distingue par sa capacité à automatiser et orchestrer la réponse aux incidents de sécurité. Là où le SIEM collecte, corrèle et détecte les événements suspects, le SOAR intervient en aval pour structurer et accélérer la gestion des alertes. Sa particularité repose sur trois dimensions :

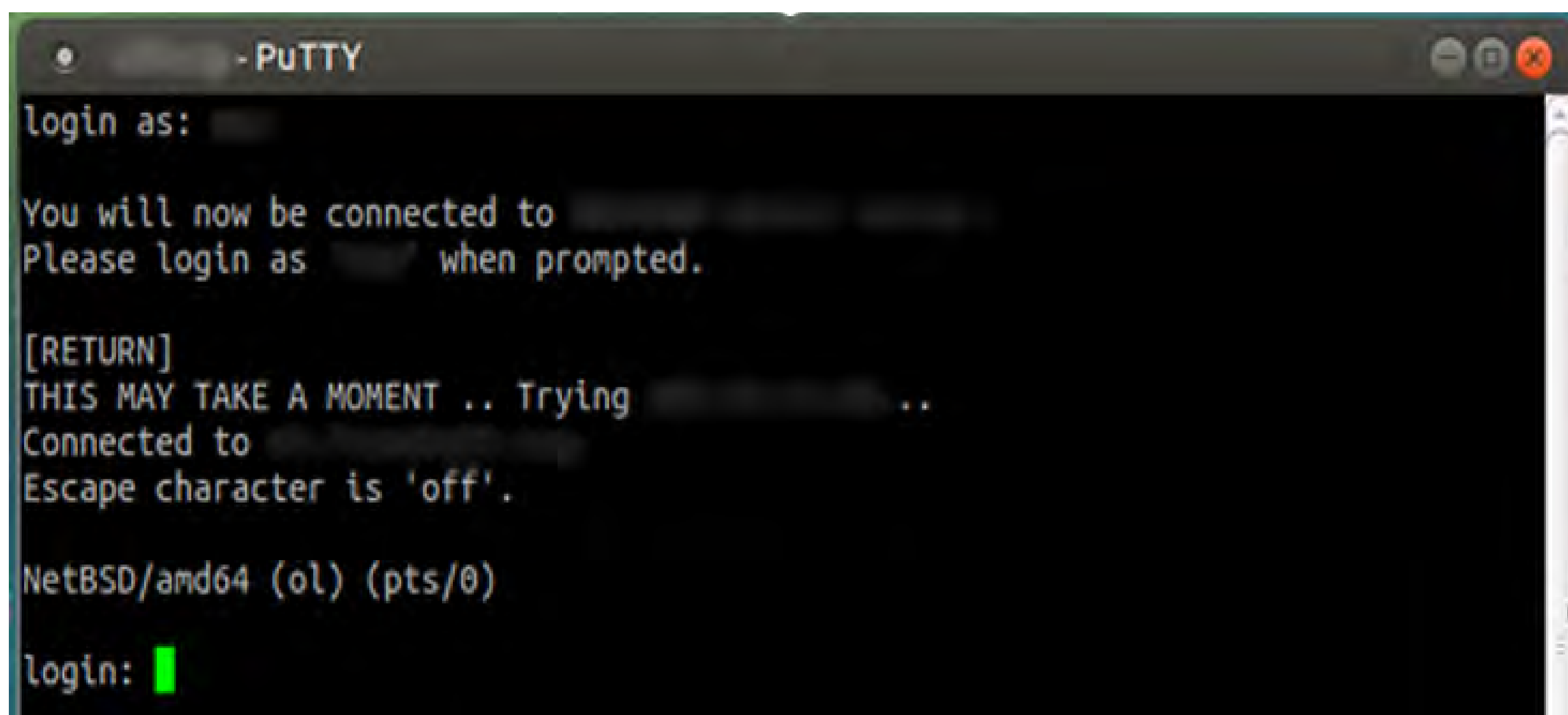
- orchestration : il interconnecte différents outils de sécurité, à savoir SIEM, [EDR](#) (*Endpoint detection and response*), pare-feu, annuaire, solutions *cloud*, afin de coordonner les actions ;
- automatisation : il exécute des *playbooks* (scénarios de réponse) permettant, par exemple, de bloquer une adresse IP, d'isoler un poste ou de désactiver un compte sans intervention humaine ;
- standardisation des réponses : il formalise les procédures d'investigation et de remédiation, réduisant les erreurs et le temps de réaction.

Le SOAR répond à une problématique clé : le volume d'alertes générées par les systèmes de détection. En automatisant leur traitement, il permet aux équipes de sécurité de se concentrer sur les incidents les plus critiques. Ainsi, le SIEM permet de voir et comprendre, tandis que le SOAR permet d'agir rapidement et efficacement face à une menace.

Cette segmentation indispensable permet d'isoler une compromission, de détecter plus rapidement une anomalie, de protéger les données sensibles, d'assurer la continuité d'activité. Un ou plusieurs événements peuvent donner naissance à une alerte, qui, si elle est confirmée, se transformera en incident. Une infrastructure mal segmentée revient à mettre tous les équipements dans une seule pièce sans cloisonnement : une intrusion se propage alors immédiatement. Dans les infrastructures numériques contemporaines, la surveillance prend donc tout son sens lorsqu'elle est mise en perspective avec le déroulement concret d'une attaque. Une cyberattaque n'est généralement pas un événement instantané : elle s'inscrit dans une succession d'actions, parfois rapides, parfois étalées dans le temps, et chacune de ces actions laisse des traces. L'intérêt pédagogique d'un tel fil conducteur est de montrer que la surveillance ne relève pas d'une observation vague ou omniprésente, mais d'une exploitation méthodique d'indices techniques (journaux, flux, événements) visant à identifier une chaîne d'intrusion et à agir avant que l'impact ne devienne majeur.

Comment se déroule une attaque ?

Imaginons une journée de fonctionnement ordinaire dans un établissement ou une organisation disposant d'un réseau segmenté, d'un annuaire d'authentification, de serveurs de fichiers, de services *cloud* et d'un dispositif de supervision centralisée. La matinée débute par un événement a priori banal : un utilisateur reçoit un courriel dont la forme semble administrative et conforme à des échanges habituels. Le message contient un lien invitant à se reconnecter. L'utilisateur saisit ses identifiants. Ce geste, fréquent et souvent non intentionnellement risqué, constitue ici le point d'entrée de l'attaque : les identifiants sont récupérés puis réutilisés depuis l'extérieur pour tenter une connexion à distance.



L'application [PuTTY](#) est un client SSH/Telnet permettant d'accéder à distance à un équipement. Il permet de se connecter à un système pour ensuite lire les *logs* en ligne de commande. Quelques minutes plus tard, la tentative d'accès se manifeste dans les journaux d'authentification. Les *logs* montrent une série d'échecs, suivie d'une réussite. Pris isolément, une connexion distante n'est pas forcément suspecte. Pourtant, d'autres éléments apportent du contexte : l'adresse IP d'origine n'a jamais été observée, la localisation est inhabituelle, et l'horaire ne correspond pas aux habitudes d'usage. C'est précisément le rôle d'une supervision centralisée : rapprocher ces signaux faibles et générer une alerte de niveau intermédiaire. À ce stade, l'attaque ne s'est pas encore traduite par des dommages visibles. La surveillance n'a pas arrêté l'événement initial, mais elle a rendu perceptible un écart significatif par rapport au fonctionnement normal.

Analysons l'extrait du journal d'authentification suivant :

```
2024-03-12 08:11:22 USER=j.dupont SRC_IP=192.168.10.45 RESULT=SUCCESS
2024-03-12 08:13:09 USER=j.dupont SRC_IP=185.243.115.78 RESULT=FAIL
2024-03-12 08:13:12 USER=j.dupont SRC_IP=185.243.115.78 RESULT=FAIL
2024-03-12 08:13:16 USER=j.dupont SRC_IP=185.243.115.78 RESULT=SUCCESS
```

On observe la nature des IP. 192.168.10.45 correspond à une adresse privée interne ([RFC1918](#)), et l'adresse 185.243.115.78 vient d'une adresse publique Internet. On observe d'abord une activité habituelle depuis le réseau interne, puis une tentative de connexion distante depuis une adresse IP publique externe. Après authentification VPN, une adresse IP interne virtuelle est attribuée à la session distante, ce qui explique que les actions internes ultérieures apparaissent avec une adresse privée. L'analyse de cette séquence suggère deux échecs rapides, puis une réussite avec la même adresse IP externe. Ce qui peut indiquer soit un test de mot de passe, ou l'usage d'identifiants compromis. L'enrichissement par géolocalisation ([GeoIP](#)) du système de supervision enrichit automatiquement l'événement. La corrélation temporelle montre deux connexions,

```
2024-03-12 08:13:16
USER=j.dupont
SRC_IP=185.243.115.78
Pays estimé=Roumanie
Ville estimée=Bucarest
Type de connexion=VPN
```

une interne en France et l'autre externe en Roumanie, ce qui constitue une impossibilité géographique, typique de l'usage d'identifiants compromis. Cependant, aucun élément isolé

```
2024-03-12 08:11:22 SRC_IP=192.168.10.45 Localisation=France (réseau interne)
2024-03-12 08:13:16 SRC_IP=185.243.115.78 Localisation=Roumanie
```

(IP étrangère, échec d'authentification, modification de groupe) ne suffit à caractériser une attaque. C'est la corrélation temporelle et contextuelle qui permet d'élever le niveau d'alerte. Lors de la tentative d'accès initiale, les journaux du service VPN conservent l'adresse IP publique d'origine de l'utilisateur distant (par exemple 185.243.115.78). Une fois l'authentification réussie, le client VPN se voit attribuer une adresse IP interne virtuelle (par exemple 192.168.10.45), qui sera ensuite utilisée dans les journaux du réseau interne, de l'annuaire et des serveurs. Il est donc normal que la première alerte fasse apparaître une IP

publique, tandis que les actions internes ultérieures soient enregistrées avec une IP privée. Dans la suite de la matinée, l'activité interne commence à changer de nature. L'accès obtenu ne suffit pas à l'attaquant : il cherche désormais à augmenter ses privilèges. On observe alors, dans les journaux système et ceux de l'annuaire, des comportements révélateurs : requêtes inhabituelles vers les services d'identité, tentatives d'accès à des ressources administratives, recherches de comptes et de groupes à privilèges. Certaines actions peuvent rester discrètes, mais d'autres déclenchent des traces explicites, par exemple une tentative de modification de groupe sensible. La surveillance joue ici un rôle clé : l'alerte générée le matin est enrichie par ces nouveaux événements. La chronologie se forme. Ce qui pouvait sembler un incident de connexion devient progressivement l'indice d'une stratégie d'intrusion.

```
2024-03-12 09:54:18
EVENT_ID=4662
USER=j.dupont
SRC_IP=192.168.10.45
ACTION=Query Active Directory
OBJECT=CN=Administrateurs_Domaine
RESULT=Success
```

Consultation inhabituelle de comptes à privilèges

```
2024-03-12 10:42:07
EVENT_ID=4728
USER=j.dupont
SRC_IP=192.168.10.45
ACTION=Add member to group
GROUP=Admin_Serveurs
TARGET_ACCOUNT=j.dupont
RESULT=Success
```

Tentative d'ajout au sein d'un groupe sensible

```
2024-03-12 10:44:11
SRC_IP=192.168.10.45
DST=192.168.30.10
PORT=3389
SERVICE=RDP
RESULT=Success
```

Accès ressources admin

On observe ici la même IP interne (192.168.10.45), attribuée lors de la session VPN, les requêtes vers l'annuaire, la consultation d'un groupe à privilèges, l'ajout du compte à un groupe administrateur, la connexion [RDP](#) (*remote desktop control*) vers un serveur interne. Individuellement, une requête AD peut être légitime et une connexion RDP peut être autorisée, mais la séquence chronologique est révélatrice. Le système de supervision

l'établit ainsi, correspondant à un schéma classique : compromission, reconnaissance, élévation de privilège, accès serveur :

Heure	Événement
08:13	Connexion VPN depuis IP étrangère
08:13	Attribution de l'IP privée 192.168.10.45
09:54	Consultation du groupe Administrateurs_Domaine
10:42	Ajout au groupe Admin_Serveurs
10:44	Connexion RDP vers serveur interne

À la mi-journée, l'attaquant passe à l'étape du mouvement latéral : après avoir compromis un compte, il cherche maintenant à se déplacer dans l'infrastructure pour atteindre les serveurs critiques. Cette phase se caractérise par une intensification de l'activité réseau détectable par les équipements de sécurité : connexions successives vers plusieurs hôtes, tentatives d'accès à des partages et requêtes répétées vers divers services.

Si la segmentation réseau limite la propagation, elle reste insuffisante sans surveillance active. La détection repose sur plusieurs indicateurs : les outils réseau identifient des comportements de reconnaissance interne et la télémétrie des postes signale des programmes inhabituels ou l'usage anormal d'outils d'administration. C'est la supervision centralisée qui, en corrélant ces différents signaux, permet d'élever le niveau d'alerte et de déclencher une décision opérationnelle : isoler le poste ou le compte compromis avant la propagation de l'attaque.

```
2024-03-12 13:17:58
SRC_IP=192.168.10.45
DST_IP=192.168.30.12
PORT=445
PROTO=TCP
ACTION=ALLOW
```

```
2024-03-12 13:18:04
SRC_IP=192.168.10.45
DST_IP=192.168.30.15
PORT=445
PROTO=TCP
ACTION=ALLOW
```

```
2024-03-12 13:18:09
SRC_IP=192.168.10.45
DST_IP=192.168.30.22
PORT=445
PROTO=TCP
ACTION=ALLOW
```

```
2024-03-12 13:18:16
SRC_IP=192.168.10.45
DST_IP=192.168.30.25
PORT=445
PROTO=TCP
ACTION=ALLOW
```

Ces éléments montrent que l'IP source 192.168.10.45 correspond au poste utilisateur compromis. Les adresses 192.168.30.x appartiennent au VLAN serveurs ; le port 445 correspond au protocole [SMB](#) (*server message block*, partages de fichiers). Les connexions successives vers plusieurs serveurs (intervalle de quelques secondes, même port, même origine). Cela correspond typiquement à une reconnaissance automatisée interne. Un poste utilisateur légitime n'ouvre généralement pas des connexions SMB vers plusieurs serveurs en moins de 30 secondes.

L'observation du journal pare-feu permet de voir les tentatives vers les services multiples :

```
2024-03-12 13:19:02
SRC_IP=192.168.10.45
DST_IP=192.168.30.10
PORT=3389
ACTION=ALLOW
```

```
2024-03-12 13:19:06
SRC_IP=192.168.10.45
DST_IP=192.168.30.11
PORT=5985
ACTION=ALLOW
```

Journalisation du pare-feu

Les ports concernés sont 3389 (RDP) et 5985 (WinRM, *Windows remote management*, administration distante). Cela signifie que le poste tente différents protocoles d'administration. L'observation de la télémétrie poste (EDR) montre que la menace tente une reconnaissance interne :

```
2024-03-12 13:17:41
HOST=PC-UTIL-23
USER=j.dupont
PROCESS=powershell.exe
COMMAND=Invoke-Command -ComputerName 192.168.30.12
```

```
2024-03-12 13:18:12
HOST=PC-UTIL-23
PROCESS=net.exe
COMMAND=net view /domain
```

Heure	Événement
08:13	Connexion VPN depuis IP étrangère
08:13	Attribution de l'IP privée 192.168.10.45
09:54	Consultation du groupe Administrateurs_Domaine
10:42	Ajout au groupe Admin_Serveurs
10:44	Connexion RDP vers serveur interne
13:17	Connexions SMB multiples
13:18	Commandes PowerShell distantes
13:19	Tentatives RDP et WinRM

Le réseau est segmenté avec les VLAN utilisateurs en 192.168.10.x et les VLAN serveurs en 192.168.30.x. Mais les règles autorisent certains flux (administration, partage). L’attaquant exploite ces flux légitimes. La segmentation limite la propagation, mais la détection comportementale est indispensable. C’est à ce niveau que le SIEM peut appliquer des règles comme :

- plus de 5 connexions SMB vers serveurs différents en moins d’une minute ;
- exécution de PowerShell suivie d’accès RDP multiples ;
- mouvement latéral précédé d’une élévation de privilèges.

Ce qui a pour conséquence une augmentation du score de risque, un passage en alerte critique et enfin un déclenchement d’isolement du poste. Face à cette corrélation, le poste 192.168.10.45 est isolé du réseau. Le compte j.dupont est désactivé. Les serveurs ciblés sont analysés. L’attaque est stoppée avant d’atteindre un hyperviseur ou un serveur de fichiers critique. Les journaux réseau révèlent qu’à partir de 13h17, le poste 192.168.10.45 établit des connexions successives vers plusieurs serveurs du segment 192.168.30.0/24 via le port 445. Cette activité est suivie de tentatives d’accès RDP et WinRM. Parallèlement, la télémétrie du poste signale l’exécution de commandes PowerShell à distance. La corrélation de ces événements avec l’élévation de privilège observée le matin constitue un indicateur typique de mouvement latéral. La supervision centralisée élève alors le niveau de criticité et permet l’isolement préventif du poste compromis. Le mouvement latéral exploite souvent des protocoles légitimes. Ce n’est pas le protocole qui est suspect, mais le comportement et sa fréquence. Dans l’après-midi, l’attaquant cherche à atteindre son objectif final, souvent lucratif : déployer un rançongiciel afin de chiffrer massivement des fichiers, perturber le service puis extorquer une rançon. Les premiers signes apparaissent rapidement dans les journaux : hausse anormale des écritures sur un serveur de fichiers, création accélérée de fichiers modifiés, multiplication de processus, parfois tentatives de compression ou de transfert sortant de données. Des connexions vers des serveurs externes peuvent aussi indiquer un pilotage à distance ou une exfiltration.

À ce stade, la surveillance devient décisive : l’alerte passe au niveau critique car elle s’appuie sur une séquence cohérente d’événements (connexion anormale, élévation de privilèges, mouvement latéral, puis activité destructive). Une réponse rapide peut alors être déclenchée : blocage des flux sortants, mise en quarantaine d’un serveur, isolation d’un poste, réinitialisation de comptes et, si nécessaire, interruption contrôlée de certains services. La surveillance des journaux du serveur de fichiers permet de voir la hausse anormale des écritures :

```
2024-03-12 15:41:12
HOST=srv-fichiers01
METRIC=WriteOperationsPerMinute
VALUE=18500
BASELINE=1200
```

Le serveur passe d’une activité normale (environ 1200 écritures/min) à un niveau très supérieur, compatible avec un chiffrement automatisé.

```
2024-03-12 15:41:29
HOST=srv-fichiers01
EVENT=FileRename
COUNT=3200
WINDOW=60s
EXTENSION=.locked
```

Le journal d’audit fait apparaître la création de fichiers modifiés.

Une vague de renommages avec extension atypique est un indicateur fréquent d’activité de type rançongiciel. La télémétrie poste montre à cet égard une multiplication de processus :

L'exécution d'un binaire inhabituel et l'explosion du nombre de processus, signe d'une automatisation et d'un chiffrement. La tentative de compression avant exfiltration est

```
2024-03-12 15:40:57
HOST=PC-UTIL-23
USER=j.dupont
PROCESS=encryptor.exe
PARENT=powershell.exe
HASH=9f1c2a...
ACTION=Executed
```

```
2024-03-12 15:41:05
HOST=PC-UTIL-23
PROCESS_COUNT_IN_30s=48
BASELINE=6
```

une option fréquente. La compression de répertoires partagés peut correspondre à une préparation d'exfiltration en double extorsion.

```
2024-03-12 15:39:44
HOST=PC-UTIL-23
PROCESS=7z.exe
COMMAND=7z a C:\Temp\archives.7z \\srv-fichiers01\partage\
RESULT=Success
```

Le pare-feu montre un transfert inhabituel :

```
2024-03-12 15:42:10
SRC_IP=192.168.10.45
DST_IP=45.144.112.9
DST_PORT=443
BYTES_OUT=3.2GB
DURATION=4m12s
ACTION=ALLOW
```

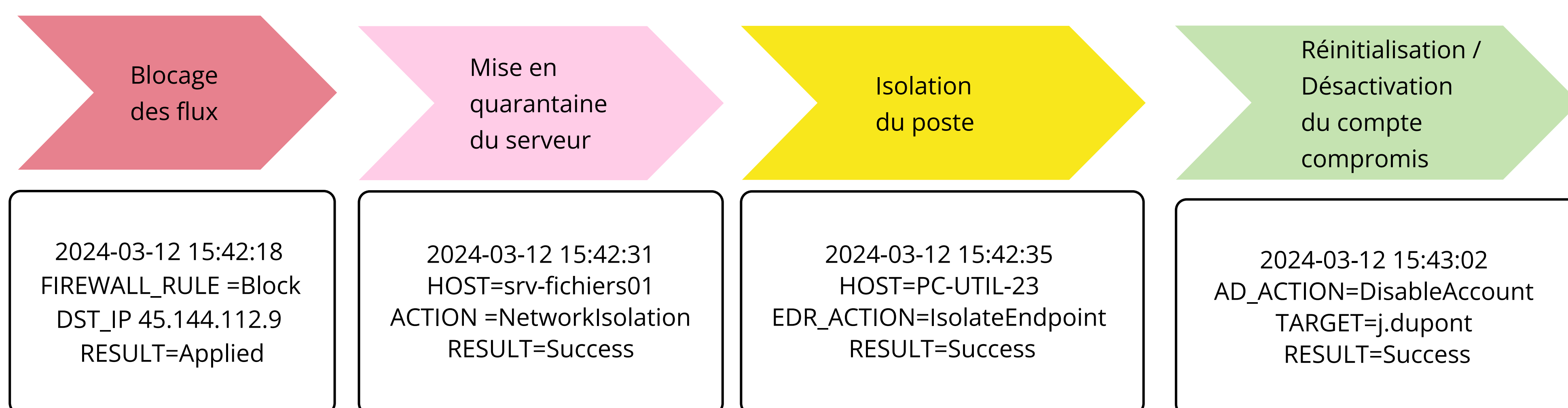
Avec les adresses IP en 192.168.10.45 pour le poste interne et 45.144.112.9 pour le serveur externe (Internet), le volume sortant très élevé sur une durée courte est l'indicateur possible d'une exfiltration. Enfin l'enrichissement GeoIP permet d'identifier la localisation du serveur externe :

```
2024-03-12 15:42:10
DST_IP=45.144.112.9
GeoIP_Pays=Pays-Bas
Reputation=Suspect (liste
interne SOC)
```

La géolocalisation IP n'est pas une donnée de *log* fiable à 100%. C'est un indicateur, non une preuve. La localisation est une interprétation (GeoIP), non un champ initial du *log*. L'alerte devient critique au regard de la chronologie suivante :

Heure	Événement
08:13	Connexion VPN depuis IP étrangère
08:13	Attribution de l'IP privée 192.168.10.45
09:54	Consultation du groupe Administrateurs_Domaine
10:42	Ajout au groupe Admin_Serveurs
10:44	Connexion RDP vers serveur interne
13:17	Connexions SMB multiples
13:18	Commandes PowerShell distantes
13:19	Tentatives RDP et WinRM
15:41	Activité destructive (écritures/renommages massifs)
15:42	Flux sortant volumineux vers IP externe

En matière de contre-mesures typiques, dès l'alerte critique, des actions peuvent être déclenchées (automatiquement ou manuellement) :



Ces mesures visent à stopper la propagation, empêcher l'exfiltration, limiter le chiffrement et préserver des preuves. L'enseignement principal est que les journaux du serveur de fichiers indiquent une hausse brutale des écritures et une vague de renommages de fichiers en quelques minutes. En parallèle, la télémétrie poste met en évidence l'exécution d'un programme inhabituel et une multiplication rapide de processus, compatible avec une activité de chiffrement. Les équipements périmétriques enregistrent simultanément un flux sortant volumineux vers une adresse IP externe, enrichie par géolocalisation. Corrélés avec les événements antérieurs (connexion anormale, élévation de privilèges, mouvement latéral), ces signaux conduisent à une alerte critique et déclenchent des mesures de confinement : blocage de flux, isolement du poste, mise en quarantaine du serveur et neutralisation des identifiants compromis.

Le SIEM est un outil de surveillance centralisée qui collecte les *logs* (journaux) provenant des serveurs, des postes utilisateurs, des pare-feu, des équipements réseau, des applications, des services cloud. Il analyse ces informations, corrèle les événements entre eux et génère des alertes en cas de comportement suspect. Sans SIEM, on a des milliers de lignes de *logs* dispersées. Avec un SIEM, le système détecte automatiquement un schéma anormal et alerte l'administrateur. Le SIEM est important car il permet de détecter plus rapidement une attaque, de reconstituer la chronologie d'un incident, de centraliser la supervision, de produire des rapports de sécurité. Il est en fait le « centre de contrôle » qui collecte toutes les traces du système d'information, les analyses et déclenche une alerte en cas de danger.

Ce scénario met en évidence un point essentiel : aucun outil isolé ne suffit à lui seul. La surveillance des infrastructures est efficace lorsqu'elle combine plusieurs sources de traces : *logs* d'authentification, journaux système, événements applicatifs, flux réseau, supervision des équipements périmétriques, et éventuellement télémétrie des postes. Ce qui permet de contrer l'attaque n'est pas la simple accumulation de données, mais la capacité à les interpréter dans une logique de corrélation et de contexte. La surveillance transforme une multitude d'événements techniques, souvent banals pris séparément, en une lecture structurée d'une intrusion en cours.

La maintenance et la surveillance des réseaux au cœur des formations CIEL

Pour l'enseignement de l'informatique et de la cybersécurité, en [baccalauréat professionnel CIEL](#) ou [BTS CIEL](#), une telle mise en situation permet de rendre visible une réalité souvent abstraite ; les attaques laissent des traces, et ces traces sont lisibles si l'on a mis en place une journalisation cohérente, un minimum de durcissement préalable, et des outils

capables de corréler et de hiérarchiser. Elle permet aussi de rappeler une idée centrale : la surveillance n'empêche pas nécessairement l'entrée initiale, mais elle réduit fortement la probabilité que l'attaque atteigne sa phase finale. En ce sens, surveiller une infrastructure revient à renforcer sa résilience : observer ce qui se passe, comprendre ce qui se passe, puis agir à temps.

Les référentiels desdits diplômes insistent particulièrement sur les aspects de la surveillance et de la journalisation pour la maintenance des différentes infrastructures. Dans le BTS CIEL, option A « Informatique et réseaux », les éléments liés à la surveillance et à la maintenance sont inscrits dans le bloc Pôle « Exploitation et maintenance de réseaux informatiques » en pages 12, 13 et 14. Les activités professionnelles liées à la supervision et à la maintenance des infrastructures informatiques et réseau font apparaître :

- le suivi de l'exploitation technique ;
- la supervision de l'état du réseau ;
- le diagnostic de premier niveau ;
- la configuration et intégration d'équipements ;
- la remontée d'alertes sur anomalies détectées.

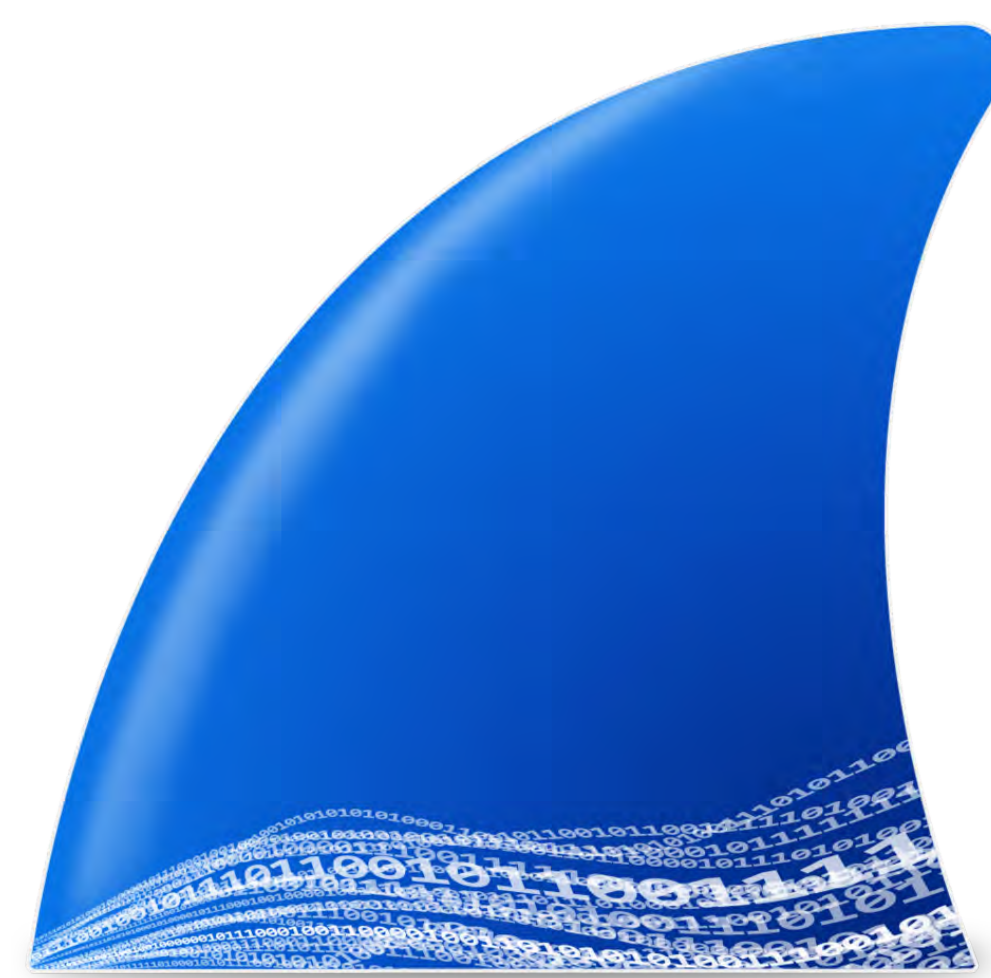
Ces activités couvrent des compétences directement associées à la lecture de journaux réseau, à l'exploitation d'un système d'information, à la surveillance des anomalies et à la réaction à des incidents, même si le référentiel n'utilise pas explicitement les mots *journalisation* ou *logs* (ces expressions sont couvertes par le terme plus large *supervision/exploitation* ou *diagnostic*).

Dans le référentiel du baccalauréat professionnel CIEL le pôle « Mise en œuvre des réseaux informatiques » inclut des activités d'exploitation et maintien en condition opérationnelle :

- l'exploitation d'une installation réseau ;
- la maintenance corrective et préventive ;
- la gestion d'incidents techniques ;
- le suivi de l'installation avec documentation et *reporting*.

Les tâches impliquent concrètement des opérations de contrôle d'état, d'interprétation d'événements, la détection d'anomalies et les actions correctives, compétences nécessaires à la lecture et interprétation de traces (*logs*, alertes).

Les textes officiels des référentiels utilisent des formulations génériques (*exploitation*, *maintenance*, *suivi de l'état du réseau*, *diagnostic*) pour décrire cet ensemble de compétences techniques. La [lecture de journaux](#), la détection d'anomalies et les actions de remédiation s'inscrit dans ce champ d'expertise surveillanciel. Les applications pédagogiques illustrant ce *monitoring* des infrastructures nécessitent une connaissance approfondie des [réseaux informatiques](#). On peut mettre en place de manière pédagogique et pratique en classe des activités de visualisations des flux avec des logiciels libres comme [Wireshark](#).



Wireshark Foundation, CC BY-SA 4.0, [Wikimedia Commons](#)

AIGRAIN, Alice, HONORÉ, Célia, 2024. La surveillance par l'image : usages, théories, résistances (XXe– XXIe siècle) », *Terminal* [en ligne], 138. [Consulté le 10 mai 2026]. Disponible à l'adresse : <http://journals.openedition.org/terminal/9724>

AïM, Olivier, 2020. *Les théories de la surveillance: du panoptique aux surveillance studies*. Malakoff : Armand Colin. Collection U.

AïM, Olivier (dir.), 2023. « Surveillance et contre-surveillance », *Quaderni*, 2023/1, 108.

AHLSTRAND, Roland, GAUTIE, Jérôme, 2018. « Lean versus Learning? Work Organization, Job Quality and the Making of Innovative Workplaces in the Aerospace Industry in France and Sweden », communication au congrès mondial de l'ILERA. [en ligne]. [Consulté le 10 septembre 2026]. Disponible à l'adresse : <https://shs.hal.science/halshs-03242211/document>

AJUNWA, Ifeoma, 2023. *The Quantified Worker: Law and Technology in the Modern Workplace*, Cambridge University Press.

BAIOCCO, Sara, FERNÁNDEZ-MACÍAS, Enrique, RANI, Uma et PESOLE, Annarosa, 2022. *The Algorithmic Management of Work and its Implications in Different Contexts*, JRC Working Papers Series on Labour, Education and Technology, 2022/02, Séville, Commission européenne, Centre commun de recherche. [en ligne]. [Consulté le 10 septembre 2026]. Disponible à l'adresse : <https://publications.jrc.ec.europa.eu/repository/handle/JRC129749>

BALL, Kristie, 2021. *Electronic Monitoring and Surveillance in the Workplace. Literature Review and Policy Recommendations*, Luxembourg, Office des publications de l'Union européenne. [en ligne]. [Consulté le 10 septembre 2026]. Disponible à l'adresse : <https://publications.jrc.ec.europa.eu/repository/handle/JRC125716>

BENTHAM, Jeremy, 1791. *Panoptique . Mémoire sur un nouveau principe pour construire des maisons d'inspection et nommément des maisons de force*, par Jérémie Bentham... [en ligne]. [Consulté le 8 mai 2026]. Disponible à l'adresse : <https://gallica.bnf.fr/ark:/12148/bpt6k114009x>

BENVEGNÙ, Carlotta, GABORIEAU, David, 2020. « Les mondes logistiques. De l'analyse globale des flux à l'analyse située des pratiques de travail et d'emploi », *Travail et Emploi* [en ligne]. 162. [Consulté le 10 septembre 2026]. Disponible à l'adresse : <https://journals.openedition.org/travailemploi/10065>

BLASCO, Sylvie, ROCHUT, Julie, ROULAND, Bénédicte, 2024. *Impact de l'intensification et de l'autonomie au travail sur la santé mentale*, DARES, « Valorisation de la recherche », 4. [en ligne]. [Consulté le 10 septembre 2026]. Disponible à l'adresse : <https://dares.travail-emploi.gouv.fr/publication/impact-de-lintensification-et-de-lautonomie-au-travail-sur-la-sante-mentale>

BOINI, Stéphanie., COLIN, Régis, LANGEVIN, Valérie, GAUTIER, Marie-Agnès, 2024. « Effets des expositions psychosociales sur la santé des salariés. Mise à jour des connaissances épidémiologiques », *Références en santé au travail* [en ligne]. 180. [Consulté le 10 septembre 2026]. Disponible à l'adresse : <https://www.inrs.fr>

CHAMAYOU, Grégoire, 2013. *Théorie du drone*. Paris : La Fabrique éditions.

CHRISTL, Wolfie, 2024. *Managing and Monitoring Mobile Service Workers via Smartphone App*. Cracked Labs. [en ligne]. [Consulté le 10 septembre 2026]. Disponible à l'adresse : https://crackedlabs.org/dl/CrackedLabs_Christl_MobileWork.pdf

COROMINES, Laure, 2025. « L'IA, nouvelle contremaîtresse au travail ». *Le Monde* [en ligne]. [Consulté le 12 septembre 2026]. Disponible à l'adresse : https://www.lemonde.fr/m-perso/article/2025/12/07/l-ia-nouvelle-contremaitresse-au-travail-c-est-la-machine-qui-dicte-la-cadence-et-favorise-la-perte-d-autonomie_6656400_4497916.html

CNIL, 2025. Mission éthique : publication du cahier air2024 « La surveillance dans tous ses états. Quelle éthique pour (protéger) nos libertés ? ». *CNIL* [en ligne]. [Consulté le 10 mai 2026]. Disponible à l'adresse: <https://www.cnil.fr/fr/cahier-air2024>

CODACCIONI, Vanessa, 2025. *Comment les Etats répriment: une courte histoire du pouvoir de punir*. Quimperlé: Éditions Divergences.

DENEUVILLE, Allan, 2025. *OSINT: enquêtes et démocratie*. Bry-sur-Marne : INA.

DENEUVILLE, Allan, LIMONIER, Kevin. « Osint, contre-enquête et terrains numériques ». *Podcast de l'université Paris 8*. Université Paris 8, 6 février 2023, 62:58. [en ligne]. [Consulté le 10 mai 2026]. Disponible à l'adresse : <https://www.podcastics.com/podcast/episode/osint-contre-enquete-et-terrains-numeriques-223515/?s=2060>

DORNE, Geoffrey, 2025. *IA ↗ NARCHIE*. HCKR.FR.

FOURMENTRAUX, Jean-Paul, 2020. *AntiDATA : la désobéissance numérique art et hacktivisme technocritique*. Dijon: les Presses du réel. Perceptions.

FOURMENTRAUX, Jean-Paul, 2023. *Sousveillance: l'oeil du contre-pouvoir*. Dijon : les Presses du réel.

GAUTIÉ, Jérôme, PEREZ, Coralie, 2023. « Le taylorisme à l'âge du numérique a investi les entrepôts logistiques », *Le Monde* [en ligne]. [Consulté le 12 septembre 2026]. Disponible à l'adresse : <https://www.lemonde.fr/emploi/article/2023/10/16/le-taylorisme-a-l-age-du-numerique-a-investi-les-entrepots-logistiques>

GONZALEZ VAZQUEZ Ignacio, FERNANDEZ MACIAS Enrique, WRIGHT Sally, VILLANI Davide, 2025. *Digital Monitoring, Algorithmic Management and the Platformisation of Work in Europe*, Luxembourg, Office des publications de l'Union européenne. [en ligne]. [Consulté le 12 septembre 2026]. Disponible à l'adresse : <https://publications.jrc.ec.europa.eu/repository/handle/JRC143072>

GHASSEMI, Mehdi, PÉREZ LAGOS, Camila, 2024. Le regard panoptique et l'art surveillance: esthétique et politique du contournement», *tic&société* [en ligne], vol. 18, 1. [Consulté le 10 mai 2026]. Disponible à l'adresse : <http://journals.openedition.org/ticetsociete/8667>

GUILLAUD, Hubert, 2026. Les guerres des drones. *Dans les algorithmes* [en ligne]. [Consulté le 2 juin 2026]. Disponible à l'adresse: <https://danslesalgorithmes.net/2026/05/28/les-guerres-des-drones>

GUILLAUD, Hubert, 2024. Vers une surveillance au travail sans limite. *Dans les algorithmes* [en ligne]. [Consulté le 2 juin 2026]. Disponible à l'adresse: <https://danslesalgorithmes.net/2024/09/03/vers-une-surveillance-au-travail-sans-limite>

HÉMEZ, Rémy, 2022. *Les opérations de déception : ruses et stratagèmes de guerre*. Paris : Perrin Ministère des armées.

HOCHSCHILD, Arlie Russell, 1983. *The Managed Heart: Commercialization of Human Feeling*, Berkeley, University of California Press.

JEMINE, Grégory, 2019. « L'outil face au manager : le contrôle du travail à l'ère du numérique, un terrain controversé ? », *Les Cahiers du numérique* [en ligne] vol. 15, n° 4, p. 137-162. [Consulté le 12 septembre 2026]. Disponible à l'adresse : <https://shs.cairn.info/revue-les-cahiers-du-numerique-2019-4-page-137?lang=fr>

LAUVIN, Rémi, 2024. *Le cinéma des formes furtives: résister en images au regard surveillant*. Paris : Éditions Mimésis.

LE DEUFF, Olivier, ROUMANOS, Rayya, 2025. *Rapport final du projet MatriosclA. MATRIce Osint pour les Cas d'usage de l'IA*. Institut des hautes études du Ministère de l'Intérieur; MICA - Media Information Communication et Art. <halshs-05404123>.

LE DEUFF, Olivier, 2021. L' Open Source Intelligence (OSINT) et les enquêtes numériques: la panoplie du maître d'armes [en ligne]. [Consulté le 2 juin 2026]. Disponible à l'adresse: <https://shs.cairn.info/revue-i2d-information-donnees-et-documents-2021-1-page-92?lang=fr>

LE DEUFF, Olivier, 2021. L' Open Source Intelligence (OSINT) comme prisme hyperdocumentaire [en ligne]. [Consulté le 2 juin 2026]. Disponible à l'adresse: <https://shs.cairn.info/revue-i2d-information-donnees-et-documents-2021-1-page-56?lang=fr>

MAUROUX, Amélie, BARADJI, Eva, DENNEVAULT, Céline, BÈQUE, Maryline, 2017. « Quelles sont les évolutions récentes des conditions de travail et des risques psychosociaux ? », *DARES Analyses* [en ligne]. 082. [Consulté le 11 septembre 2026]. Disponible à l'adresse : <https://dares.travail-emploi.gouv.fr/publications/quelles-sont-les-evolutions-recentes-des-conditions-de-travail-et-des-risques>

KELLOGG, Katherine C., VALENTINE, Melissa A., CHRISTIN, Angèle, 2020. « Algorithms at Work : The New Contested Terrain of Control », *Academy of Management Annals* [en ligne] vol. 14, n° 1, p. 366-410. [Consulté le 11 septembre 2026]. Disponible à l'adresse : <https://journals.aom.org/doi/10.5465/annals.2018.0174>

LEDIT, Guillaume. Propagations. *YouTube* [en ligne]. [Consulté le 25 juin 2026]. Disponible à l'adresse: https://www.youtube.com/channel/UCNzkaIBiFBfW84o2O_13OeA

LEVY, Karen, 2023. *Data Driven: Truckers, Technology, and the New Workplace Surveillance*, Princeton University Press.

LEVY, Karen, BAROCAS, Solon, 2018. « Refractive Surveillance: Monitoring Customers to Manage Workers », *International Journal of Communication* [en ligne]. vol. 12. [Consulté le 11 septembre 2026]. Disponible à l'adresse : <https://ijoc.org/index.php/ijoc/article/view/7041>

MERCIER, Arnaud, 2025. *Les mots de la désinformation et de la manipulation*. Toulouse : Presses universitaires du Midi. Les mots de, 43.

MEYER, Vincent, DIARD, Caroline, ROST, Dounia, 2022. « Télétravail et formes de contrôle émergentes : le cas du secteur bancaire et financier pendant la crise sanitaire de la Covid-19 », *Annales des Mines – Gérer et comprendre* [en ligne]. 149, p. 35-46. [Consulté le 11 septembre 2026]. Disponible à l'adresse : <https://shs.cairn.info/revue-gerer-et-comprendre-2022-3-page-35>

MILANEZ, Anna, LEMMENS, Annikka, RUGGIU, Carla, 2025. « Algorithmic Management in the Workplace: New Evidence from an OECD Employer Survey », *OECD Artificial Intelligence Papers*, [en ligne]. 31. [Consulté le 11 septembre 2026]. Disponible à l'adresse : https://www.oecd.org/en/publications/algorithmic-management-in-the-workplace_287c13c4-en.html

MITCHELL, Melanie, 2021. *Intelligence artificielle: triomphes et déceptions*. Malakoff: Dunod. Quai des sciences.

MOLNAR, Adam, 2025. *Surveillance and Algorithmic Management at Work: Capabilities, Trends, and Legal Implications*, Office of the Information and Privacy Commissioner of Ontario. [enligne]. Disponible à l'adresse: <https://www.ipc.on.ca/en/resources/research-hub/surveillance-and-algorithmic-management-at-work>

PCA-STREAM, 2025. Eyes on the street. Mesurer la captation de la donnée urbaine. *STREAM STUDIES* [en ligne]. N° 1. [Consulté le 10 mai 2026]. Disponible à l'adresse : https://www.pca-stream.com/wp-content/uploads/2025/04/STREAM-STUDIES_EYES-ON-THE-STREET.pdf

POURÉ, Clément, 2025. *Les nouveaux contremaîtres : enquête sur la surveillance au travail à l'heure de l'IA*. Paris : Éditions des Équateurs.

SCHELLMANN, Hilke, 2024. *The Algorithm: How AI Decides Who Gets Hired, Monitored, Promoted, and Fired*, New York, Hachette Books.

TAYLOR, Frederick Winslow, 1911. *The Principles of Scientific Management*, New York et Londres, Harper & Brothers.

TRÉGUER, Félix, 2024. *Technopolice: la surveillance policière à l'ère de l'intelligence artificielle*. Quimperlé: Éditions Divergences.

TRONTO, Joan C., 2009. *Un monde vulnérable: pour une politique du care*. Paris: Éd. la Découverte.

ZUBOFF, Shoshana, 1988. *In the Age of the Smart Machine: The Future of Work and Power*, New York, Basic Books.

Bureau de l'accompagnement des usages et de l'expérience utilisateur DNE - TN3



dne.lettre-edunum@education.gouv.fr

Vous recevez cette lettre car vous êtes abonné
aux Cahiers ÉduNum thématiques.

Souhaitez-vous continuer à recevoir les Cahiers
ÉduNum thématiques ?

Abonnement/Désabonnement

À tout moment, vous disposez d'un droit d'accès,
de rectification et de suppression des données qui
vous concernent (articles 15 et suivants du RGPD).
Pour consulter nos mentions légales, [cliquez ici](#).

ISSN 2739-8846 (en ligne)



@Edu_Num