NUMÉRIQUE

CAHIER DU

Citoyenneté & Participation

Table des matières

Sommaire

Introduction

Outil extraordinaire et symbole de liberté d'expression qui a nourri tous les espoirs d'un monde meilleur, Internet montre aujourd'hui ses limites. Le tout-au-numérique, imposé ou choisi, pose effectivement de plus en plus question à nombre de citoyens et citoyennes, ce dont nous sommes témoins dans nos ateliers d'éducation permanente. C'est pourquoi nous avons décidé de rédiger un cahier consacré à différentes limites et problématiques liées à cette course au numérique.

En premier lieu, nous avons choisi de mettre en évidence ses limites démocratiques et de mettre en exergue celles qui nous semblaient particulièrement importantes. Car si Internet était au départ décentralisé, il est rapidement devenu un outil géré principalement par des géants, que sont les GAFAM, NATU et autres BATX, aux algorithmes opaques et aux finalités plus vénales que philanthropiques. Les petits génies de la Sillicon Valley sont passés du statut de stars du cool et de la liberté à celui de milliardaires avides de monopole et d'argent. Ils disent se battre pour la liberté d'expression, mais leur fortune repose sur un capitalisme de surveillance. Leur soif de données personnelles les amène à investir des sommes pharaoniques dans le métavers, le cloud, l'intelligence artificielle, le commerce électronique, l'hyper-connectivité, les systèmes d'exploitation, la publicité instantanée géolocalisée, la diversification des réseaux sociaux, les voitures autonomes hyper connectées... Ils rassemblent ainsi des informations sur nos comportements, notre travail, nos goûts, nos revenus, nos déplacements, nos fréquentations, nos origines ethniques, notre religion, nos opinions politiques, nos répertoires téléphoniques, nos agendas ou encore les publicités sur lesquelles nous cliquons. Ces données peuvent être exploitées par des publicitaires, et sont aussi très convoitées par les cybercriminels. L'insatiable appétit de ces géants s'immisce dans tous les pans de notre vie, en connectant le plus possible nos appareils et comportements : montre, surveillance du sommeil, voitures intelligentes, villes intelligentes, lunettes intelligentes, cafetière intelligente... On laisse en effet à leurs algorithmes la programmation de nos relations, de nos consommations, de notre information, notamment avec des assistants vocaux. Et désormais les GAFAM s'intéressent à notre santé, des données parmi les plus sensibles qu'ils convoitent, misant sur l'intelligence artificielle que ce soit pour optimiser les traitements dans les hôpitaux, pour ce qui est de Google, surveiller des états de santé, via l'Apple Watch, ou encore ouvrir des pharmacies en ligne pour Amazon. Ces géants monopolistiques vont jusqu'à défier les États et les démocraties, en ne se soumettant pas à leurs lois et en propageant la désinformation, comme nous le verrons dans l'étude de Philippe Courteille *Les dangers démocratiques du numérique*. Cette concentration de pouvoir suscite des préoccupations croissantes en matière de confidentialité, d'antitrust, de désinformation et même d'influence politique. Cela pousse les régulateurs du monde entier, en particulier en Europe, à renforcer les législations pour encadrer leurs pratiques. Dans un premier temps, nous allons faire un petit tour d'horizon des dangers démocratiques qui se dessinent face à la numérisation de nos vies, de plus en plus gérées par des algorithmes dont on ne sait quasi rien.

Malgré cette concentration opaque des pouvoirs, des élus n'hésitent pas à confier à des algorithmes, la gestion de certains aspects des sciences humaines, comme la recherche d'emploi ou la répartition d'allocations sociales. Dans son analyse, *Numérisation du recrutement et de l'orientation- Promesses et conséquences des algorithmes*, Edgar Gillet nous montre que dans toute dématérialisation, on constate invariablement une part de déshumanisation car la neutralité des algorithmes n'existe pas.

Mais le technosolutionnisme reste le nouveau dada des économies libérales ... tout comme des États moins démocratiques. Désinvestir dans l'humain pour investir dans les algorithmes reste une grande tentation pour nos services publics. Dans sa publication *Smart cities : obsolescence à programmer ?*, Benoît Debuigne s'intéresse ainsi au concept des villes intelligentes et à l'idée en vogue de la gestion automatisée de divers pans urbanistiques. Que ce soit pour la mobilité, les économies d'énergie, la gestion des déchets ou de l'éclairage public, les idées fusent dans la tête des futuristes modernes. Mais, si le phénomène a le vent en poupe dans certaines mégalopoles asiatiques, nous verrons que les communes belges sont plus hésitantes. Car finalement, le jeu en vaut-il la chandelle ?

Et puis, avons-nous les moyens de nos ambitions numériques ? Dans un premier temps, Boris Fronteddu interrogera le concept de données personnelles à travers son analyse *Donner ses données*. Peut-on, de manière réaliste, continuer indéfiniment à collecter celles de bientôt huit milliards d'habitants et les stocker dans des data centers de plus en plus énergivores ? Les géants de la tech ont en effet réussi à se rendre indispensables au fonctionnement de l'économie et, plus largement, de la société, de son infrastructure jusqu'aux services publics les plus essentiels. S'agit-il de collecter nos données pour faciliter notre prise en charge lors d'une hospitalisation ou pour nous proposer une livraison de fast food à l'heure précise où le sentiment de faim commence à nous parcourir ? Dans un cas comme dans l'autre, il est urgent de démocratiser cet enjeu en commençant avec une question fondamentale : est-ce bien utile et si oui, à qui ? Dans sa seconde analyse, *La matérialité de la « double transition » - Jusqu'où vont-ils descendre ?*, Boris Fronteddu s'intéresse aux limites matérielles de la croissance numérique. Il se penche, dans ce cadre, sur la consommation de métaux par l'industrie numérique et aux conséquences environne-

mentales de ce qui s'apparente à une fuite en avant extractiviste. L'Union européenne, pauvre en exploitations minières de ce type sur son sol, pense désormais à exploiter les fonds marins, ce qui amène à de nombreuses questions qui pèsent autour de l'impact environnemental et climatique d'une telle entreprise. Jusqu'où sera-t-on prêt à descendre au nom de la « double transition » ?

D'autant qu'aujourd'hui, l'intelligence artificielle est en train de multiplier les besoins énergétiques du numérique. « *D'ici 2030, les centres de données européens qui développent l'intelligence artificielle auront besoin de trois fois plus d'énergie, selon une étude du consultant McKinsey* »[1] du premier novembre 2024. Une IA aujourd'hui accessible à tous, notamment pour créer des deepfakes, hypertrucages en français, qui permettent de copier un son, une écriture, une photo ou une vidéo avec une précision de plus en plus déconcertante. Un outil particulièrement en vogue pour imiter, tromper, arnaquer, influencer ou racketter, qui n'est pas sans danger, comme nous le démontre Philippe Courteille dans son étude *Deepfakes, le mensonge à l'ère de l'intelligence artificielle* et qui explose en Belgique. Il est en effet possible aujourd'hui de faire dire ou de faire faire quelque chose à n'importe qui dans un audio, une image ou dans une vidéo. À l'ère de la désinformation et des fake news, cette étude tente de percevoir les risques qu'engendre cette nouvelle façon de mentir et de tromper les citoyens.

Face à une autre inquiétude, souvent évoquée lors de ses ateliers en éducation permanente, Roxane Lejeune s'est intéressée aux conséquences de cette course au numérique sur la santé des citoyens, qu'elle soit physique ou psychologique, à travers son analyse *Toutes et tous devant les écrans, quels effets pour notre santé ?*. Même si nous manquons encore de recul face à une multitude d'innovations, finalement assez récentes, Roxane Lejeune tente de dresser un bilan des dangers et des craintes qui animent de plus en plus de citoyen·ne·s.

Nous tenterons enfin, de réfléchir à une possible sobriété numérique avec l'étude d'Anna Constantinidis *La sobriété numérique, au-delà des idées reçues*. Face à cette surenchère consumériste et énergivore, une des solutions nous paraît résider dans la sobriété numérique, à savoir un horizon sociétal, collectif, dans lequel on interroge les besoins et où on démocratise les questions liées au numérique et où celui-ci serait donc pensé collectivement à la hauteur des enjeux qu'il soulève. La sobriété numérique est en effet un horizon sociétal et collectif, plus qu'une démarche individuelle.

En tant qu'association d'éducation permanente, il nous semble urgent que ces questions sociétales, environnementales et démocratiques, face à une numérisation entendue par les pouvoirs publics et privés sans aucune consultation populaire, deviennent accessibles au plus grand nombre. C'est dans cet esprit que nous avons écrit ce cahier, car ces questions légitimes méritent d'être traitées par un maximum d'acteurs, dans tous les secteurs possibles, pour faire en sorte que ce tsunami numérique, apparemment irréversible, soit mis en question. Et qu'à tout le moins, un réel débat public sur le sujet devienne possible, que les citoyen·ne·s aient leur mot à dire pour que les outils numériques restent des outils démocratiques utiles et non un nouveau Far West subi. Comme l'écrivait Romain Gary « *Il faut toujours connaître les limites du possible. Pas pour s'arrêter, mais pour entreprendre l'impossible dans les meilleures conditions* ». Or aujourd'hui, qui connaît vraiment les limites du numérique ?

[1] Agence Belga, « L'utilisation d'électricité pour l'IA en Europe va tripler d'ici 2030, selon une étude », Le Vif, le 1er novembre 2024, [en ligne :] https://datanews.levif.be/actualite/lutilisation-delectricite-pour-lia-en-europe-va-tripler-dici-2030-selon-une-etude/, consulté le 3 novembre 2024.

Philippe Courteille est licencié en journalisme et communication de l'ULB. Il a travaillé comme journaliste-réalisateur freelance pour de nombreuses émissions de télévision pendant 25 ans. Il est aujourd'hui responsable de la thématique Médias & Actions citoyennes chez Citoyenneté & Participation.

Philippe courteille

Les dangers démocratiques du numérique

Introduction

Indéniablement, le numérique a ouvert de nouveaux champs des possibles et des libertés. Que ce soit pour s'informer, apprendre et découvrir, avec un accès aux sources d'informations de toute la planète, pour répondre à la plupart des questions qu'on peut se poser. Une nouvelle liberté de communiquer, de créer, de se former, de s'émerveiller, de travailler à la maison, de gagner du temps, d'être livré à domicile, de s'exprimer de diverses manières… Faut-il encore le préciser, Internet a tout révolutionné jusqu'à permettre à des peuples de se soulever en Égypte, en Tunisie ou à Hong-Kong.

Mais ces nouvelles libertés sont, comme souvent, confrontées à de nouveaux excès. Ceux-ci sont dus, nous le verrons, à différents facteurs comme le fonctionnement des outils, l'impréparation de leurs propriétaires et à la soif de pouvoir et de monopole des GAFAM, BATX[1] ou NATU[2], à une complexité technologique croissante, à l'expression du vice et de la malveillance contenue jusqu'ici par des lois élaborées pendant des siècles ou encore à la naïveté de divers dirigeants. Des excès désormais boostés à l'IA, à se demander si le monde n'a pas ouvert une boîte de Pandore qu'il est désormais compliqué de maîtriser, ou si, à tout le moins, nous ne mettons pas la charrue avant les bœufs dans de nombreux domaines.

Comment empêcher les citoyens de se faire aspirer leur vie privée ?

Ces problèmes pourraient-ils faire vaciller certains pans des démocraties ? C'est ce que nous allons voir à travers diverses problématiques qui posent désormais question et auxquelles tentent de répondre l'Union européenne et nos gouvernements non sans mal. Car bien sûr il s'agit de réguler le web, mais de nombreux freins l'empêchent. Comment parvenir à réguler un système algorithmique dont on ne connaît pas les programmations, réalisées de surcroît, aux États-Unis ou en Chine, pays régis par des lois différentes ? Comment faire plier des géants quasi monopolistiques, détenteurs d'outils dont les populations ne peuvent plus se passer ? Comment réguler des arnaques lancées depuis des contrées antipodales, en toute impunité ? Comment empêcher les citoyens de se faire aspirer leur vie privée, via les fameuses données personnelles, malgré eux ? Comment circonscrire le déluge de mensonges, de harcèlements et de violences ? Comment faire comprendre aux citoyens que leurs réseaux sociaux, leur ordinateur, leur smartphone, leurs jeux vidéo, leur domotique, même leur montre ou leur cafetière connectée, et bientôt leur voiture et même leurs lentilles de contact[3] ou leurs lunettes, sont autant d'espions au service du commerce et de la propagande, avec des garanties de sécurité aléatoires ? Les questions sont multiples et manquent cruellement de réponses. Nous allons tenter de les mettre en exergue et d'en comprendre différents dangers que des accords internationaux devront réguler à tout prix, dans des délais les plus courts possibles.

À se demander parfois si la course au numérique n'est pas en train, mine de rien, de dépasser l'immense majorité des habitants de notre planète. Citoyens, politiques, fonctionnaires, employés de tout secteur, jeunes et autres, beaucoup pensent comprendre ce qu'il se passe et gérer la situation. Et pourtant.

Un "Dêmos" démotivé pour un "kratos" craqué

Au départ, le mot démocratie nous vient du grec ancien « dêmos », c'est à dire le peuple, et « Kratos », le pouvoir. Le pouvoir au peuple, traduit par la participation citoyenne à l'élection de ses représentants. Un pouvoir par le peuple et pour le peuple. Pierre Rosanvallon écrivait sur la démocratie qu'elle était à la fois une promesse et un problème[4]. Une promesse, dans le sens où elle ne peut jamais être satisfaisante. Et un problème, parce qu'il faut toujours trouver des réponses nouvelles pour répondre à l'idéal qu'elle incarne. Or aujourd'hui, le numérique bouscule sérieusement de nombreux pans démocratiques. Non seulement les cordons sanitaires volent en éclats, mais les propagandes mensongères attisent la haine vis-à-vis des politiques, et même des journalistes, de par le monde. Comment en est-on arrivé là ? Comment l'émotionnel a-t-il à ce point surpassé le sens du collectif et le rationnel dans les débats ?

Comment peut-on faire confiance aux maîtres de la Silicon Valley – qui tentent de contourner les lois à des fins principalement mercantiles, ne paient pas leurs impôts ou font faire des travaux inhumains et mal payés à des modérateurs de contenus ou à des personnes qui cliquent sur des photos pour entraîner les IA – plutôt qu'en nos personnalités politiques démocratiquement élues et en nos journalistes censés être des gages de vérité ?

Pour le comprendre, il faut d'abord pénétrer la logique de fonctionnement des géants du numérique, devenus quasi incontournables, ce qui n'est pas sans conséquences.

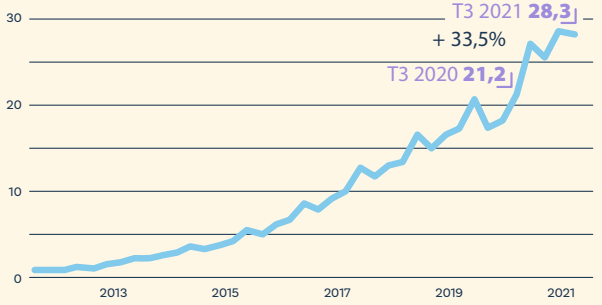
1. Quand les GAFAM, BATX et autres NATU, imposent leur fonctionnement

a. Éthique vs business

« *En 1996, Sergeï Brin et Larry Page, 23 et 24 ans, créent un algorithme de classement des sites internet à la logique simple : plus une page reçoit de visites, de clics, plus elle est considérée comme pertinente et bien référencée. Google est né. En 2004, Mark Zuckerberg, 20 ans à peine, et ses copains créent un réseau social sympa pour communiquer entre "amis" : Facebook. Points communs de Sergeï, Larry, Mark et leurs compères : ils sont jeunes, ils sont idéalistes, ils croient en la liberté et aux vertus du Premier amendement, le Free Speech, qui interdit de limiter la liberté de parole. Le succès de Google et de Facebook est vertigineux* ». Voilà notre introduction dans notre étude dédiée à la propagation des fake news sur Internet[5]. Depuis 1996, la course aux clics a vite profité aux messages provocants et aux réactions émotionnelles, épidermiques, faisant du faux et de l'excessif des produits bien plus rentables que la vérité et la nuance. C'est le premier point de bascule, aux multiples conséquences politiques et médiatiques notamment.

Au-delà de ce modèle de fonctionnement, aux innombrables conséquences absurdes, le modèle économique de ces jeunes « dans le vent », s'est très vite appuyé sur la publicité. Un système d'annonces mondialisé à la rentabilité inouïe. Selon le documentaire *Le piège du clic*, de Peter Porta[6], le chiffre d'affaires de la publicité en ligne dépasserait celui de tous les supports et médias cumulés, soit quatre cents à cinq cents milliards de dollars.

La croissance des revenus publicitaires de Facebook



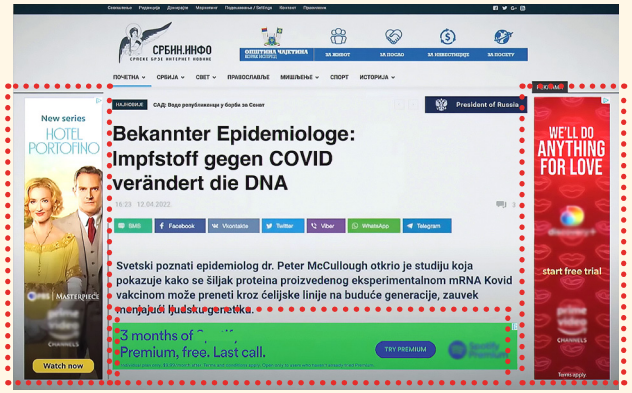
Source : statista

Au centre, les géants Google et Facebook, ou plutôt Alphabet et Meta, leaders mondiaux dès leur création, qui se sont partagés longtemps l'essentiel des rentrées publicitaires. De son côté, la presse mondiale a vu ses rentrées publicitaires fondre. Dès 2016 « *Alan Rusbridger, l'ancien rédacteur en chef du Guardian, a accusé Facebook d'avoir aspiré près de 20 millions de livres de revenus publicitaires sur les 100 millions escomptés par le journal britannique cette année-là* »[7], et on parle là d'un géant de la presse. Le quatrième pouvoir, qui respecte la déontologie journalistique, gage de vérification des faits, se retrouve en concurrence directe avec toutes sortes de sites et de pseudo médias, qui ne respectent aucune garantie de vérité. Le quatrième pouvoir, ce vérificateur de faits, subit un coup dont il ne se remettra jamais complètement.

b. Vous avez dit publicités ciblées ?

Car la publicité ciblée fut l'argument massue. Amener la publicité sur un produit auprès de la personne qui effectue une recherche sur ce produit, c'est imparable face aux publicités dans des mass médias, qui diffusaient justement de la publicité de masse. Et ce à l'échelle planétaire de surcroît. Difficile de résister à un tel rouleau compresseur : les annonceurs étaient sous le charme.

Pourtant, cet argument a commencé à prendre un peu de plomb dans l'aile quand des annonces ont été découvertes sur des sites complotistes, xénophobes voire violents, auxquels ne souscrivaient pas du tout les annonceurs. L'opacité algorithmique montrait ses limites. Un exemple parmi d'autres : un site russe annonçant que les vaccins contre le Covid-19 modifieraient l'ADN humain. À gauche et à droite de l'écran, des publicités pour la marque de vidéos en ligne Amazon Prime. Plus une bannière pour Spotify. L'algorithme ne s'est basé que sur le nombre de vues de ce site, sans aucune vérification de crédibilité. Le client, lui, ne sait donc pas sur quel genre de site sa publicité aboutit.



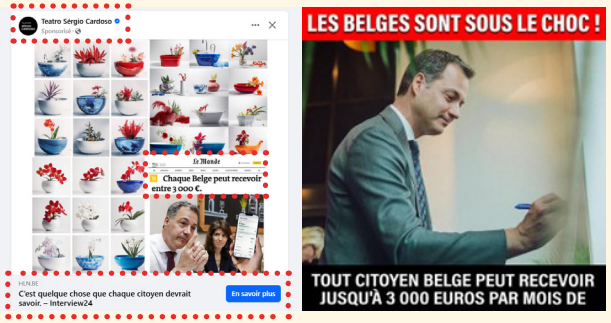
Source : Image tirée du documentaire « Le piège du clic », de Peter Porta, diffusé dans l'émission Doc Shot sur la Une, RTBF, le 13 juin 2024 à 22h35.

Ainsi, n'importe quelle pub pouvait être exposée sur un site de propagande.

Le pot-au-rose a été dénoncé dès 2016 par Jammi Nandini, une jeune femme qui travaillait dans le marketing. Un jour son patron lui demande de faire une campagne de pubs sur Google Ad, qui annonce toucher des clients potentiels dans le monde.

L'annonce est alléchante et Jammi Nandini rêve déjà de voir sa publicité diffusée sur des sites comme CNN ou le *Washington Post*. Quelle ne fut pas sa stupéfaction de découvrir la publicité sur le site de Breitbar, un journal de l'alt-right[8] américaine, considéré comme suprémaciste et complotiste. Le site était rempli de pubs de grandes marques. Madame Nandini a alors prévenu toutes ces marques, captures d'écran à l'appui, que leurs annonces faisaient la promotion de l'extrême droite et aidaient celle-ci à se financer. Breitbar touchant effectivement jusqu'à huit millions de dollars de revenus via ces pubs. La réaction de ces marques est immédiate et en trois mois, le site perd 90 % de ses revenus publicitaires. Jammi Nandini, sera co-fondatrice du groupe Sleeping Giants qui continue de dénoncer ce genre de pratique. Cet exemple est très révélateur de l'ineptie algorithmique de Google qui, rappelons-le, diffuse de la publicité sur 90 % des sites qui en affichent. Ainsi, ces messages publicitaires sont affichés sur des sites en fonction de leur audience, comprenant, bien sûr, nombre de sites mensongers, puisque la désinformation est rentable dans le système Google. Aucune éthique, aucune transparence, juste une rentabilité maximale au nom de la liberté d'expression et de commerce. Tout cela a-t-il changé depuis 2016 ? Ce serait logique que ces maîtres du web aient pris conscience de leur manque de sérieux, ou oserait-on dire d'éthique, en ce qui concerne leurs placements publicitaires. Pas si sûr.

Car du côté de Meta, ce sont carrément de fausses publicités, mais de vraies arnaques que l'on peut trouver sur Facebook. En juillet 2024, nous recevions des dizaines d'annonces promettant des gains magiques grâce à l'IA et/ou à la cryptomonnaie sur notre page Facebook. Celles-ci utilisaient, sans leur consentement, l'image de personnalités de la télé, du cinéma, et même de la politique avec un Alexander De Croo annonçant un gain de trois mille euros pour tous, glissé par exemple, dans un faux article du journal *Le Monde*.



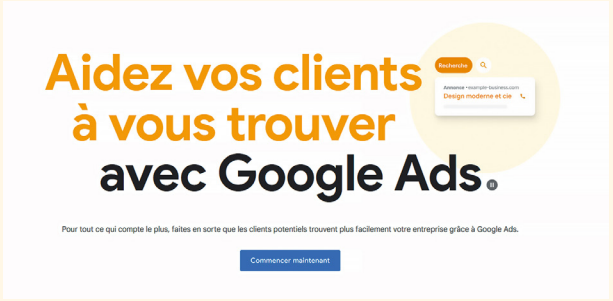
Source : ces deux captures d'écran ont été réalisées sur Facebook en juillet 2024

Virginie Efira, Gad Elmaleh, François Debrigode, Elise Lucet… Ils sont parfois même associés à un deepfake, une vidéo ou un audio manipulé, où on les voit promettre des rentrées d'argent aussi plantureuses que magiques. Et comble du comble, quelle ne fut pas notre surprise de voir encore, en juillet 2024, un Mark Zuckerberg expliquer dans une annonce qu'en investissant dans sa cryptomonnaie, on pouvait gagner cinq cents euros par jour. La vidéo est un deepfake et sa cryptomonnaie, Libra, a été vendue en 2022. Mais le plus incroyable, c'est que cette fausse pub était diffusée… sur Facebook. Même le propre patron de la plateforme n'a pas de contrôle de son image sur son propre réseau social…. Que rajouter ?

Source : capture d'écran réalisée sur Facebook en juillet 2024

Quelle confiance accorder à des groupes qui ne cherchent pas à maîtriser leurs outils ? Il apparaît évident que pour Meta, comme pour Alphabet, l'éthique, et même la crédibilité, passe après les milliards de dollars de rentrées publicitaires. Et plus vous allez cliquer sur des arnaques, plus l'algorithme vous en fournira, des dizaines, parfois même en une seule journée. Bref, quand les al-

gorithmes trouvent un « pigeon », tous les arnaqueurs du genre peuvent avoir l'opportunité de le cibler. Si on met cette histoire en lien avec le slogan de Google, « Aidez vos clients à vous trouver avec Google Ads », ça en serait limite drôle si ce n'était aussi déplorable.



Source : capture d'écran de la page de présentation du site Google Ads : https://ads.google.com/intl/fr_ca/home/

C'est d'autant plus choquant que ces géants du net prétendent récolter les données personnelles de leurs membres pour leur offrir… un service pertinent. Grâce à des centaines, voire des milliers, de datas récoltées, Alphabet et Meta connaissent nos vies, nos goûts et prétendent même pouvoir anticiper nos envies, et c'est à l'utilisateur de signaler les arnaques sur Facebook. À l'heure actuelle, le débat est toujours en cours entre l'UE et Meta pour faire respecter les règles en matière de données personnelles, de marchés numériques de services numériques.

Notons également les possibilités d'achats en ligne, et de livraison à domicile, de produits illicites comme des contrefaçons, des médicaments ou des stupéfiants, à l'instar de celle-ci, reçue sur… Facebook :

Source : capture d'écran réalisée en juillet 2024 sur Facebook. En Belgique, le cannabis à fumer contenant moins de 0,2 % de THC est considéré depuis 2019 comme un "autre tabac à fumer". Il est soumis à la même législation que le tabac (taxe, emballage, etc.). La limite est donc fixée à 0,2 %, soit 125 fois moins que la dose écrite sur cette publicité en ligne.

Fin juillet 2024, une enquête du *Wall Street Journal* souligne que : « *Méta diffuse des publicités sur Facebook et Instagram qui orientent les utilisateurs vers des marchés en ligne pour les drogues illégales, des mois après que le Wall Street Journal ait rapporté pour la première fois que le géant des médias sociaux faisait face à une enquête fédérale sur la pratique* »[9]. « *Petite précision : ces publicités frauduleuses ne sont en aucun cas cachées, étant donné qu'elles sont répertoriées publiquement dans la Bibliothèque de Publicités Meta*[10]*. Meta met alors en avant sa solution : payer un abonnement pour accéder à Facebook ou Instagram. De cette manière, si un utilisateur paye, il sera exempt de la publicité, et donc des contenus sponsorisés frauduleux. Cependant, s'il ne paye pas chaque mois, il devra accepter cette situation. "Payer ou consentir", il faut choisir* »[11].

c. Une cupide éthique

En 2021, Frances Haugen, ancienne employée de Facebook, confirme cette priorité de la logique vénale chez Meta. Elle divulgue des dizaines de milliers de documents internes de la compagnie (« Facebook Files ») à la Securities and Exchange Commission (SEC) et au *Wall Street Journal*. Sous le nom Facebook Papers, cette affaire montre le manque de contrôle du réseau social sur les contenus qui circulent sur sa plateforme, du discours de haine à l'incitation à la violence, en passant par les fake news[12].

C'est même à des ONG, des journalistes ou des associations de lutte contre la fraude de révéler les pots-aux-roses au public. Exemple, le 11 juillet 2024, un nouveau rapport, publié par l'ONG de défense des médias Qurium, dénonce une gigantesque campagne de désinformation du réseau russe Doppelgänger : « *Pour déjouer la vigilance de Facebook ou de Twitter, qui déploient des filtres pour bloquer automatiquement ces publications, Doppelgänger a mis en place un système qui repose, entre autres, sur l'achat en continu de dizaines de milliers de noms de domaines. Chacun d'entre eux n'est utilisé que quelques jours durant, le temps de rediriger les internautes vers des sites de propagande, avant d'être abandonnés une fois détectés … Ils ne servent pas seulement à republier de faux articles du Point, du Parisien ou du Monde, mais aussi à amplifier l'audience des vidéos ou articles créés par d'autres acteurs ayant des liens plus ou moins distendus avec les autorités russes* »[13]. En 2023 déjà, « *l'ONG Reset Tech avait identifié un vaste réseau composé de plus de 242 000 fausses pages Facebook, dont une petite partie était utilisée pour diffuser des publicités frauduleuses. Derrière se cachait vraisemblablement un acteur proposant, clé en main, des pages Facebook nécessaires au montage de campagnes et d'arnaques* »[14]. Les réseaux sociaux sont ainsi utilisés à des fins criminelles et propagandistes et on voit mal, que ce

soit Meta ou X, comment leurs propriétaires pourraient réguler ces phénomènes. Si toutefois ils en ont l'intention. Exemple avec les vidéos postées par des enfants sur YouTube, qui continuent de susciter l'intérêt de pédophiles. S'il est évidemment complexe pour Google d'empêcher des enfants de poster des vidéos sur YouTube, il n'est en revanche pas normal que ses algorithmes continuent d'alimenter ces odieux personnages en images similaires et que des commentaires parfois très explicites, comme lorsque des pédophiles suggèrent les moments les plus « croustillants » d'une vidéo, ne soient pas repérés, dénoncés aux autorités et poursuivis[15]. Ce qui a fait réagir Alphabet lors d'un de ces scandales en 2019 ? Le départ d'annonceurs importants, et donc la perte de grosses sommes d'argent. Un « nettoyage » du réseau a été opéré à ce moment-là, mais les algorithmes continuent de fonctionner de la même façon. Ce qui incite à se poser la question de l'esprit qui anime les élites de chez Alphabet.

L'exemple de Guillaume Chaslot est très éclairant à ce sujet. Il est expert en IA et en datasciences et, de 2010 à 2013, il a travaillé dans l'équipe chargée de l'algorithme de recommandation de YouTube, chez Google à Los Angeles. À l'époque, il constate que les algorithmes de YouTube, enferment les utilisateurs dans ce qu'on appelle « une bulle informationnelle ». En clair, si vous regardez des vidéos complotistes, l'algorithme vous en enverra de plus en plus, au point que vous aurez une impression de vérité ou de légitimité, tellement vous en êtes inondés. Guillaume Chaslot se rend également compte que les vidéos complotistes sont massivement recommandées car elles génèrent du temps de vue. « *Dans mon travail, j'ai essayé de proposer plusieurs systèmes de recommandations de contenus qui permettaient à l'utilisateur de découvrir de nouveaux contenus, de découvrir d'autres points de vue* »[16], des contenus autres que complotistes. Mais Google n'était pas intéressé. Pire. « *Mon manager m'a dit : "Attention, je ne continuerais pas à travailler là-dessus, si j'étais toi"* ». Il obéit mais, six mois plus tard, Guillaume Chaslot n'y tient plus et y revient car pour lui c'est du pur bon sens. Il est licencié. Il fonde alors AlgoTransparency pour informer sur le fonctionnement des algorithmes de YouTube. Sur la page de présentation de son site, on peut lire :

> Dans le monde d'aujourd'hui, l'intelligence artificielle contrôle ce que le monde regarde. Il promet de vous apporter des informations et des divertissements particulièrement pertinents. L'objectif réel de l'algorithme est toutefois de maximiser le temps de visionnage. Cela l'amène à favoriser le contenu sensationnaliste et les pièges à clics. À l'échelle du monde, ce biais algorithmique amplifie la désinformation, polarise le débat public et promeut les contenus préjudiciables. La mission d'AlgoTransparency est d'exposer l'impact des algorithmes les plus influents. Notre priorité est centrée sur YouTube, qui recommande 700 millions d'heures de vision par jour[17].

Rappelons que YouTube est « *la 2e plateforme sociale la plus utilisée dans le monde (2,49 milliards d'utilisateurs actifs mensuels), derrière Facebook (3 milliards)* »[18].

Ce qu'ont montré Frances Haugen et Guillaume Chaslot est clair : chez Meta et Alphabet, la priorité est l'argent et rarement l'éthique, la morale ou encore la bienveillance. Et, même si certains aspects restent complexes dans la programmation des algorithmes, notamment les notions de nuances, comme lorsque Facebook, voulant censurer la nudité, censurait également des œuvres d'art, Guillaume Chaslot nous montre que les algorithmes peuvent clairement être améliorés.

d. Un risque de bulle spéculative

Autre phénomène dont on parle finalement peu : quelle est l'efficacité des publicités ciblées ? En effet Google facture des vues mais constate elle-même que 56,1 % de ses publicités sont « invisibles » (une publicité est considérée comme visible si 50 % de ses pixels sont visibles pendant une seconde)[19]. Bref, 56,1 % des gens y prêteraient peu attention. Tim Hwang, ancien employé de Google, chercheur et auteur du livre *Le grand krach de l'attention*, affirme que les publicités en ligne sont peu efficaces, notamment à cause des bloqueurs de pubs, des usurpations de domaines, des fermes à clics[20] ou encore par l'attitude elle-même du « consommateur » de la pub. Le taux de clics sur les bannières serait ainsi dérisoire, « *de l'ordre de 0,01 %* »[21]. Nous devons bien avouer que la pertinence des publicités reçues sur nos réseaux ne nous semble pas très élevée, à titre tout à fait personnel. M. Hwang cite également le cas de Procter & Gamble, l'un des plus gros annonceurs au monde, qui « *a décidé en 2017 de retirer 200 millions de dollars de son budget marketing digital pour le réinjecter dans de la publicité plus classique. Ce qu'ils ont découvert, c'est qu'il n'y a eu absolument aucun changement sur leurs ventes, leurs revenus, ni les comportements d'achats de leurs clients… Pourtant le marché de la publicité en ligne continue de croître, alimentant une bulle spéculative que Tim Hwang compare à celle des subprimes, à l'origine de la crise financière de 2008. Tôt ou tard, elle pourrait exploser et faire des dégâts* »[22]. On peut en effet imaginer un retrait massif des annonceurs, qui pourraient même réclamer des dommages pour mensonges sur l'efficacité des publicités ciblées. Des pertes massives de rentrées publicitaires, moteur principal de Google et de Meta et de leurs projets, pourraient causer bien des soucis à ces derniers. À moins que l'IA et leurs datas ne les sauvent. Mais côté UE, le Comité européen de la protection des données (EDPB) a demandé fin 2023 l'interdiction de l'utilisation non consentie des

données personnelles d'usagers à des fins de publicité ciblée[23]. Affaire à suivre.

e. D'autres modèles, pas beaucoup plus vertueux

Pour ce qui est des autres géants du net, ce ne sont pas les réseaux chinois, contrôlés par leur gouvernement, qui nous garantissent plus d'ouverture d'esprit et d'éthique. Personne ne sait ce que le parti communiste chinois fait des données récoltées sur Temu, Ali Baba ou TikTok par exemple. En tous cas, fin 2023, TikTok était condamné à « *une amende de 345 millions d'euros en Europe pour ne pas avoir protégé les données de ses utilisateurs* »[24], et spécialement celles des ados. TikTok est réputé pour avoir les algorithmes les plus performants au monde pour ce qu'on appelle l'économie de l'attention, c'est à dire nous faire rester le plus longtemps possible sur le réseau en nous proposant des vidéos qui excitent notre curiosité. C'est donc un acteur majeur dans la lutte pour préserver notre vie privée et dans l'accaparement des recettes publicitaires.

Ces sociétés captent la valeur sans la rémunérer

Et que dire d'Uber qui a donné naissance à un nouveau terme, *ubérisation*. La tactique est simple, rendre son application incontournable dans un pays, y changer les pratiques (tout en ignorant les règles locales, le plus longtemps possible, et en cassant le marché)[25] avant de faire changer les règles et les lois, à leur avantage. La journaliste Laura Encinas résumait assez bien la situation dans un de ses articles : « *En tant que protagonistes du numérique et/ou des nouvelles technologies, ils déconstruisent - ou "disruptent" - les schémas de l'économie traditionnelle, dynamitant des secteurs qu'on croyait indéboulonnables (taxis, hôtels, agences de voyage…NDLR) en se plaçant notamment comme intermédiaire incontournable entre les consommateurs et les prestataires de services. Le grand méchant Natu fait peur car il dissimule les piliers de la précarisation connectée qu'une certaine techno béatitude rend possible sur fond de simulacre d'économie collaborative. Quand les chantres de ce phénomène affirment que cela redonne du pouvoir au consommateur et répond à l'évolution de ses pratiques numériques, d'autres sont plus sceptiques. C'est le cas de Michel Bauwens, théoricien belge de la révolution peer-to-peer, pour qui "Facebook, YouTube ou Google relèvent de l'hypercapitalisme, car ce sont des sociétés qui produisent", tandis qu'"Uber ou Airbnb sont plutôt des formules parasitaires, dans la mesure où ces sociétés captent la valeur sans la rémunérer"* »[26]. Des livreurs, dirigés par des machines et cotés par des clients, parfois mécontents du service de livreurs débordés et exploités. Pire, en France, on a même vu les franchises Uber Eats sous-traitées à des sans-papiers par des citoyens, qui se réservaient une part du maigre salaire. Le cynisme est total.

L'ubérisation, technique éprouvée par AirBnB, Deliveroo ou encore Booking.com (« *Le leader mondial de la réservation d'hébergements en ligne se nourrit du bénéfice des hôteliers. Mais il fait également disparaître une partie des recettes du secteur Horeca. Au détriment, notamment, du fisc belge* »[27]). Tout cela réalisé de manière automatique, souvent depuis l'étranger, tout en trouvant le moyen de payer un minimum de taxes et d'impôts. Ce système manque clairement de réglementation, constitue une concurrence déloyale importante et une dépendance à ces plateformes. Ils font ainsi tous du commerce dans notre pays en limitant au maximum leur participation au budget de l'État et aux outils démocratiques que sont les administrations, les écoles ou les aides publiques. Le site économique français Capital estimait qu'en 2020, Google n'avait payé que « *20,5 millions d'euros d'impôts sur les bénéfices en France, soit dix fois moins que ce qu'il aurait dû payer s'il déclarait au fisc français ses revenus effectivement générés dans l'Hexagone* »[28]. Il s'agit donc d'un manque à gagner important, non seulement pour nos entreprises, mais aussi pour les pouvoirs publics, et d'un affaiblissement supplémentaire de nos démocraties, après le siphonage des rentrées publicitaires, notamment pour la presse, essentielle à l'équilibre démocratique. On peut aussi parler des plateformes de streaming, comme Netflix, Amazon Prime, Disney, Apple TV+ et autres HBO Max, qui affaiblissent radicalement les audiences de nos productions télévisuelles ou cinématographiques.

f. Un bras de fer musclé pour faire respecter les lois

Que penser de leurs positions dominantes, voire monopolistiques ? En Europe et même aux États-Unis c'est un bras de fer permanent pour faire respecter aux géants du numérique les lois de la concurrence. Le 5 juillet 2024 encore, lors d'une décision rendue par un juge de Washington, Alphabet a été reconnu coupable de pratiques anticoncurrentielles concernant son moteur de recherche, notamment via des contrats l'imposant comme logiciel par défaut sur des appareils. « *Le juge a estimé que, "après avoir étudié attentivement les témoignages et les preuves, la cour est arrivée à cette conclusion : Google est un monopole et a agi de manière à maintenir ce monopole"* »[29]. « *Le groupe de Mountain View (Californie) était accusé d'avoir versé des dizaines de milliards de dollars, jusque 26 milliards de dollars uniquement l'année dernière, pour s'assurer que son moteur de recherche était celui par défaut sur un certain nombre de smartphones et de navigateurs internet, l'essentiel de cette somme étant versée à Apple. "Les accords de distribution signés par Google préemptent une part im-*

portante du marché des moteurs de recherche et empêchent ses rivaux d'opportunités pour venir le concurrencer", a justifié le juge dans sa décision »[30].

L'Europe est en lutte avec les géants du numérique depuis longtemps. Après le RGPD, le Règlement général de protection des données sorti en 2018 après six ans d'âpres négociations[31] (surtout avec les lobbies), elle a mis en application en 2023 le DMA, pour Digital Markets Act, qui impose aux géants du numérique une série d'obligations et d'interdictions permettant d'endiguer des pratiques anticoncurrentielles et le DSA, pour Digital Services Act, qui régule non seulement l'e-commerce mais aussi les contenus illicites (haineux, pédopornographiques, terroristes…) et les produits illicites (contrefaits ou dangereux) proposés en ligne. Plus de dix mille plateformes en ligne opèrent en effet sur le marché européen du numérique, estime la Commission européenne[32], même si seule une toute petite partie d'entre elles capterait l'essentiel de la valeur générée par ces activités. Des lois qui servent de modèles au monde entier. Car il apparaît extrêmement difficile de réguler ces mastodontes. Le DSA a finalement été accepté, bon gré mal gré, par les GAFAM.

Depuis leur création, ces groupes ne cessent de croître, de racheter d'autres entreprises pour devenir plus incontournables encore et récolter des milliards de données personnelles. Microsoft possède Skype, Edge, Outlook, Nokia, les réseaux sociaux Yammer et LinkedIn, et deux cent trente-six autres sociétés, achetées en trente ans. Plus fort encore, en vingt-trois ans, Alphabet s'est offert deux cent dix-sept entreprises comme YouTube, Motorola, Deepmind (IA), Waze, NestLabs (domotique) et surtout Android. Ce dernier est le système d'exploitation mobile le plus utilisé au monde sur les smartphones et les objets connectés, ordinateurs comme les télévisions (Android TV), les voitures (Android Auto), les Chromebook (Chrome OS qui utilise les applications Android) et les smartwatch (Wear OS). Désormais, les meilleurs IA publiques appartiennent aux GAFAM.

Le RGPD montre ses limites

De quoi récolter un nombre inouï de données personnelles, et ce malgré le RGPD. De quoi augmenter un peu plus leur pouvoir et imposer leurs algorithmes, rendus toujours plus efficaces.

2. De la démocratie à la datacratie

Au-delà de la passionnante publication de Boris Fronteddu, *Donner ses données*[33], nous souhaitons apporter quelques précisions sur les aspects démocratiques de cette course aux datas que nous vivons désormais au quotidien. Malgré l'obligation de demander l'acceptation des cookies, beaucoup de personnes, rencontrées lors d'ateliers EP ou de formations, ne différencient pas les cookies optionnels des autres et les acceptent car « c'est plus facile », d'autant que l'accès est parfois refusé dans le cas contraire. Les lois sont une chose mais leur compréhension et leur bonne utilisation par les citoyens en est une autre. Leur surprise est même immense quand nous leur montrons que leurs données peuvent être partagées avec des centaines d'autres entreprises et que même si une donnée est anonyme, le cumul de quelques-unes permet de les retrouver à terme. Le RGPD montre ses limites.

Aujourd'hui des sociétés continuent d'aspirer et d'utiliser nos données personnelles pour réfléchir à notre place à nos besoins et à notre cartographie mentale de consommateur. Une collègue d'une trentaine d'années, pourtant vigilante sur ses datas, reçoit depuis quelques temps des publicités pour des produits pour bébés, sur ses réseaux sociaux, comme pour lui signifier que son horloge biologique tourne. « *De quoi je me mêle aurait grommelé un de mes aïeuls !* ». En fonction de vos achats, de vos recherches en ligne ou de vos clics, les algorithmes tentent de prévenir vos besoins. Ces plateformes du numérique réfléchissent à notre place et nous renvoient à un univers dystopique orwellien qu'on n'imaginait pas possible il y a trente ans, et qui est à nos portes. Tout cela, bien sûr, présenté comme bénéfique pour tous. Des systèmes qui semblent même faire rêver certaines entreprises, voire certains technocrates et techno solutionnistes fascinés par la vidéo-surveillance, la reconnaissance faciale, la biométrie et autres illusions de sécurité absolue. Des technocrates qui ont souvent peu de remords par ailleurs, à laisser leurs citoyens se débrouiller sur un web contaminé par la vénalité, la malveillance, le mensonge, la complexité, l'opacité… Comment cela est-il possible ? Tout simplement parce qu'Internet permet de réduire les coûts un peu partout et de déresponsabiliser le plus possible ses services. Mais le net est entre les mains de sociétés monopolistiques, qui ont imposé leurs propres règles et leurs propres logiques de fonctionnement. Les patrons de plateformes passent souvent pour des gens cools, épris de liberté et de bienveillance, mais leurs actes les contredisent régulièrement.

a. "Moi, mais je n'ai rien à cacher !"

Bien sûr personne n'a rien à cacher. Ni sa manière de rouler un peu trop vite en voiture, ni la participation de son enfant au harcèlement d'un·e élève de sa classe, ni la liste exhaustive de tous les lieux et les personnes qui sont fréquentées, ni ses opinions

politiques, ni son homosexualité, ni ses mensurations, ni ses sites pornographiques préférés et ses types de fantasmes, ni le fait que son couple batte de l'aile, ni son traitement contre une MST ou une propension à la flatulence ou à la mauvaise haleine, ni des photos d'une soirée un peu « bad trip », ni une amitié hypocrite, ni son avis sur son patron, ni sa consommation d'alcool ou de cigarettes, ni ses analyses d'urine, ni son goût pour la malbouffe, ni la liste de tous ses achats en ligne, ni que les photos de ses enfants à la plage intéressent de nombreux pédophiles… Et pourtant, cette phrase, « Je n'ai rien à cacher », nous l'avons tous entendue au moins une fois. Elle souligne le décalage des personnes qui se font siphonner adresse, répertoire téléphonique, agenda, numéro de compte, numéro de registre national, photos de famille, amis ou encore répertoire téléphonique… D'ailleurs, pour les spécialistes de la question, le problème ne vient souvent pas d'une donnée isolée, même si elle peut déjà être embarrassante, mais du croisement de plusieurs données qui amènent à des conclusions intéressantes pour les annonceurs et les diffuseurs, voire des gouvernements. Nous nous rappelons cette coordinatrice d'un CPAS, accro aux réseaux sociaux, qui nous disait faire attention à bien se protéger. Quelle ne fut pas sa surprise de découvrir plus de cinq mille cookies sur son smartphone, en quelques clics dans ses paramètres. Imaginez que, selon une étude de 2021 de la School of Computer Science & Statistics de Dublin, même au repos, Android et iOS (l'autre système d'exploitation, utilisé, lui, sur les iPhones) envoient vos données à Apple et Google[34]. Les citoyens accepteraient-ils que leur vie de famille, leurs déplacements, leurs fréquentations, leurs photos privées soient utilisées et revendues par les services publics ? Alors pourquoi une telle confiance dans des entreprises étrangères ? On le sait, les entreprises du Web sont avides de nos données personnelles, car elles les revendent à prix d'or, ou les utilisent pour nous servir de la publicité ciblée. Mais beaucoup d'utilisateurs n'imaginent pas à quel point elles circulent. Une personne qui accepte de donner son numéro de téléphone à une société en ligne, a-t-elle conscience qu'elle pourrait ensuite recevoir des coups de fil publicitaires intempestifs pour profiter d'une promotion ou de conseils qu'elle n'a jamais demandés ?

Les smartphones sont les plus efficaces espions au monde

Les smartphones sont les plus efficaces espions au monde, avec une vaste opacité sur les récoltes des données. Mais selon une étude française de trois ans, réalisée par la CNIL[35] et l'INRIA[36] en 2014 : « *Entre un quart et un tiers des applications accèdent à la localisation. Mais ce qui retient l'attention, c'est la fréquence d'accès. Ainsi, une application de service de réseau social a pu accéder 150.000 fois en trois mois à la localisation d'un de nos testeurs. Cela représente un accès en moyenne par minute. Certaines applications qui ont obtenu l'autorisation (générique) d'accéder à la localisation ne se privent donc pas de l'utiliser, même lorsque l'application n'est pas visible à l'écran* »[37]. Des milliards de données vendues, partagées entre partenaires mais aussi détournées voire volées. Un trafic énorme, qui fait régulièrement fi de toute morale, éthique ou même de toute autorisation. Ainsi « *la société Meta … a été condamnée à une amende record de 1,2 milliard d'euros par la Data Protection Commission (DPC), le régulateur irlandais de la vie privée. Une somme sans précédent à l'échelle de l'Union européenne, qui surpasse de loin celle que l'entreprise Amazon avait été condamnée à verser en juillet 2021, qui était à l'époque de 746 millions d'euros* ». La DPC, « *reproche au réseau social d'avoir continué à transférer des données personnelles de ses clients européens vers les États-Unis. En 2020, la Cour de justice de l'union européenne (CJUE) avait estimé que la possibilité réservée aux services de sécurité américains de pouvoir accéder aux données des Européens était incompatible avec le droit de l'Union européenne en matière de protection des données* »[38]. 2022, *Le Monde* titrait : « *Données personnelles : des associations européennes de consommateurs portent plainte contre Google. Selon elles, Google, au moment de proposer la création d'un compte, compliquerait volontairement le refus de la collecte des données personnelles* »[39]. Un bras de fer permanent qui démontre combien les plateformes font fi du RGPD, ou, à tout le moins, ne sont pas capables de le respecter.

Et que dire du vol ? Qui en est à l'abri à part peut-être les banques avec des systèmes comme SWIFT[40] ? Même les GAFAM et les BATX :

- 2019, chez Meta, plus d'un demi-milliard de personnes, excusez du peu, ont été touchées par un piratage de données. Des numéros de téléphone, des adresses, des dates de naissance, des biographies et des adresses électroniques ont été diffusés publiquement suite à cela[41].
- Même WhatsApp, aux messages codés qui avaient rassuré bien des sceptiques, n'est pas à l'abri. En août 2024, des « *cybercriminels ont réussi à accéder à une base de données contenant des informations sensibles liées aux utilisateurs belges de WhatsApp. Ces données, désormais en vente sur un forum du Dark Web, peuvent être exploitées à des fins malveillantes* »[42]. Trois million deux cent mille utilisateurs belges en ont été victimes, près d'un quart de notre population.
- LinkedIn, qui appartient à Microsoft, a également subi un vol de données important. Les informations de plus de cinq cent millions de ses utilisateurs ont été extraites de la plateforme et proposées à la vente en ligne. L'ensemble de données comprend des informations sensibles telles que des adresses électroniques, des numéros de téléphone, des informations sur le lieu de travail, des noms complets, des identifiants de compte, ou encore des liens vers des comptes de médias sociaux. LinkedIn n'a ainsi pu protéger les données de 92 % de ses utilisateurs.

Ce vol est intervenu quelques jours après celui de Facebook[43].

- Et on se rappelle tous du Datagate en 2013. Un certain Edward Snowden, employé de la NSA, fait circuler dans les pages du *Guardian* et du *Washington Post* une série d'informations mettant en évidence l'existence d'un programme de surveillance massive déployé aux États-Unis. Ce programme de surveillance violait la vie privée de millions de citoyens. Les révélations d'Edward Snowden ont en effet soulevé pour la première fois de sérieuses questions sur la vie privée et l'utilisation des données sensibles.
- Citons bien sûr la plus impressionnante : vingt-six milliards de données[44]. Cette *mother of all breaches* (MOAB, la mère de toutes les brèches) « *révélée par Bob Dyachenko, chercheur en cybersécurité et propriétaire de SecurityDiscovery.com et l'équipe de Cybernews. Ce ne serait rien d'autre que la plus grande compilation de données qui a fuité… Et si beaucoup de ces données ne sont pas forcément neuves et qu'il y a probablement aussi des doublons, cela n'a rien d'anodin… Plus inquiétant encore la fuite comprend également des enregistrements de diverses organisations gouvernementales aux États-Unis, au Brésil, en Allemagne, aux Philippines, en Turquie et dans d'autres pays* »[45].

Et à chaque visite sur le net, nos moindres actions sont partagées avec des centaines de partenaires. Sauf si on refuse mais beaucoup de sites ont tendance à complexifier les possibilités de « non » au partage de données et faciliter le « oui », en un seul clic.

Bien malin celui qui peut vous dire où se trouvent ses données personnelles. D'autant que des *data brokers* vendent des données personnelles de gens qui ne sont même pas au courant. À qui sont-elles vendues ? Des arnaqueurs, sans doute. Des gouvernements, certainement (cfr Snowden). Des spécialistes du marketing, c'est évident.

Mais le but principal officiel : vous combler. Entendez, vous bombarder de publicités, sur votre smartphone (avec géolocalisation, proposition de promotions en direct en fonction de votre localisation, coups de fil intempestifs de call-centers…).

Et avec l'explosion de l'IA, les possibilités se multiplient. Exemple avec une des dernières idées géniales offertes aux annonceurs, comme s'il en manquait, lancée en juillet 2024 par Elon Musk, et qui s'appelle Trend Genius[46]. Les annonceurs peuvent choisir des mots-clés liés à des événements ou des sujets auxquels ils souhaitent être rattachés. Trend Genius surveille les conversations en temps réel et déploie les publicités lorsque les mentions de ces mots-clés augmentent. Une surveillance continue de vos conversations pour y placer des publicités, dites « pertinentes », et ce dans la milliseconde.

La démocratie résistera-t-elle à la tentation de l'hyper-surveillance

Les GAFAM, se partagent également la part du lion dans le cloud, cet espace qui garde vos données sur un serveur extérieur. Avec Amazon Web Services, le numéro un mondial, Microsoft Azure, Google Cloud, Salesforce (numéro un des logiciels de gestion de clients pour les entreprises) et Oracle, ces géants américains drainent, à eux seuls, un tiers des investissements. Sur le seul segment des infrastructures (IaaS), le duopole n'est pas loin : les firmes de Jeff Bezos et Bill Gates captent les deux tiers du marché, et la moitié si l'on intègre les plates-formes (PaaS)[47].

Et que dire des données biométriques, utilisées pour ouvrir son téléphone ou des applications de reconnaissance faciale, qui menacent au passage les droits les plus élémentaires à la vie privée et à l'égalité. Si la reconnaissance faciale est connue chez Facebook, pour reconnaître les membres du réseau, quelle ne fut pas la surprise du grand public en 2020, en découvrant l'existence de la société Clearview, grâce à une enquête du *New York Times*[48]. « *À l'aide d'un outil automatisé parcourant le Web, Clearview récolte toutes les images détectées comme contenant des visages humains (plus de 10 milliards de photos stockées à ce jour), et permet à ses clients, grâce à son algorithme de reconnaissance faciale, d'identifier les individus apparaissant dessus. Elle stocke aussi toute information liée à ces photos, notamment le lien URL de la page où elles se trouvent - qui contient souvent des noms et autres informations personnelles. Objectif officiel : aider la police à identifier des criminels* ». En 2021, la société américaine de reconnaissance faciale voulait tout simplement « *s'associer avec neuf pays européens dont l'Italie, la Grèce et les Pays-Bas avant que le projet soit avorté par les autorités européennes* »[49]. La tentation des autorités nationales de se munir de nouveaux outils de surveillance est un exemple frappant des dérives sécuritaires et techno-solutionnistes qui se sont emparées de différents États européens. « *La police allemande a par ailleurs utilisé des vidéos de manifestation pour retrouver des individus qui avaient manifesté lors du G20 en 2019* »[50]. Pourra-t-on encore manifester librement, à l'avenir, sans être fiché via la reconnaissance faciale, la géolocalisation, et le traitement par intelligence artificielle ? La démocratie et ses représentants résisteront-t-ils à la tentation de l'hypersurveillance ? Que devient la notion de vie privée dans un monde hyperconnecté, surtout quand on ne sait même pas où se trouvent nos données ? Des multinationales qui se comportent donc d'une telle façon qu'aucun État démocratique, aucun service public, n'en aurait le droit. Enfin presque. À Singapour, on peut trouver désormais des robots en rue, censés aider les citoyens et qui sont devenus des postes de surveillance de leurs comportements, même la nuit, observant si personne ne fume en public, ne jette un papier par terre, gare son vélo de manière incorrecte ou vend des marchandises illégalement.

Une tendance qui s'est accélérée ces dernières années alors que Singapour a l'un des taux de criminalité les plus bas au monde. Dans cette ville-État, on peut même trouver normal de placer des caméras de surveillance dans des classes pour que les parents puissent voir si le professeur donne bien cours.

Parmi les pays non démocratiques, citons l'exemple de la Chine et de son crédit social[51], généralisé dans certaines villes, qui permet non seulement la surveillance des comportements des citoyens mais ceux-ci peuvent en plus être cotés et récompensés ou punis par le gouvernement, y compris, bien sûr, les opposants au régime.

Et pendant que la puissance de ces plateformes monopolistiques et du *big data* fait rêver certains techno-solutionnistes, voire certains politiques, il est essentiel de souligner que les décisions et programmations de ces mêmes plateformes ont aussi des conséquences politiques et démocratiques, parfois dramatiques.

3. Politique, droits de l'Homme et géants du Net

Depuis l'affaire Cambridge Analytica, dont nous parlions dans notre étude sur la propagation des fakes[52], on sait que les réseaux sociaux peuvent être utilisés de façon malveillante pour influencer une élection ou un référendum. Que ce soit par le vol d'identité, le siphonage de données et la propagation de fausses informations. Mais on entend peu parler des influences de ces géants dans des guerres, des massacres ou des ingérences politiques. Ici encore, Meta est régulièrement pointé du doigt, notamment par Amnesty International.

« *D'après une enquête publiée dans le Washington Post, le PDG Mark Zuckerberg est intervenu personnellement dans des décisions ayant eu des conséquences réelles désastreuses, par exemple quand Facebook a cédé aux demandes du gouvernement vietnamien de censurer les dissidents anti-gouvernementaux* »[53]. « *Selon les informations d'un rapport de transparence de Facebook, après avoir accepté de censurer les publications antigouvernementales, la société a bloqué plus de 2200 publications d'utilisateurs vietnamiens entre juillet et décembre 2020, contre 834 les six mois précédents* ». « *Seulement quelques mois avant d'intervenir au Viêt-Nam, le fondateur avait prononcé un discours à l'université de Georgetown, dans lequel il avait déclaré estimer que Facebook "devait continuer à se battre pour la libre expression"* ». Quand le chiffre d'affaires de Facebook au Vietnam est estimé à un milliard de dollars, il semble difficile de se mettre à mal avec le gouvernement du pays.

Les conséquences dramatiques de l'amateurisme lucratif de Meta

Le cas du Myanmar est particulièrement instructif sur les conséquences dramatiques de l'amateurisme lucratif de Meta.

« *En 2017, des Rohingyas ont par milliers été tués, torturés, violés et déplacés dans le cadre de la campagne de nettoyage ethnique menée par les forces de sécurité du Myanmar. Dans les mois et les années ayant précédé ces atrocités, les algorithmes de Facebook ont intensifié la vague de haine contre les Rohingyas, contribuant ainsi à la survenue de violences dans la vraie vie* » déclarait Agnès Callamard, secrétaire générale d'Amnesty International. « *Pendant que l'armée du Myanmar commettait des crimes contre l'humanité contre les Rohingyas, Meta tirait profit de cette caisse de résonance créée par ses algorithmes qui a induit une hausse vertigineuse du sentiment de haine* ». Car pour de nombreux Birmans, le réseau social était l'unique service internet accessible, et Facebook y amplifiait considérablement les messages violents[54]. Selon une enquête de Reuters, les problèmes en Birmanie étaient anciens, et Facebook, avait été alerté à plusieurs reprises par des ONG et des experts depuis 2013[55]. Malgré ces avertissements, Facebook a continué de compter essentiellement sur les signalements d'utilisateurs et sur un seul modérateur parlant birman en 2014, puis quatre à la fin 2015, pour gérer les messages remontés par les 7,3 millions d'utilisateurs dans le pays à l'époque. Un petit effort en effectif car en 2014, « *un billet viral sur Facebook avait provoqué une explosion de violences mortelles entre des groupes bouddhistes et musulmans dans la ville de Mandalay. Le billet affirmait à tort que deux hommes musulmans étaient coupables du viol d'une jeune fille bouddhiste dans la ville. Les émeutes qui ont suivi ont conduit les autorités birmanes à bloquer temporairement Facebook, reconnaissant le rôle clé joué par la plateforme dans « l'instigation » de ces violences. Pourtant, les efforts de Meta pour répondre à cet avertissement dramatique ont été plus qu'insuffisants* »[56]. Plus incroyable encore, le réseau social avait largement recours à des modérateurs ne parlant pas birman, et donc dépendants d'outils de traduction automatique. Or ces outils fonctionnent mal avec le birman. Dans un exemple mis en avant par Reuters, une phrase disant qu'il faut « tuer tous les kalars [terme insultant désignant les Rohingya] de Birmanie, aucun ne doit rester en vie » est traduite par l'outil automatisé de Facebook en « il ne faut pas qu'il y ait d'arcs-en-ciel en Birmanie ». Sans parler des caractères d'écriture birmans qui sont difficiles à reconnaître pour les algorithmes.

Dans un communiqué, Facebook affirme cependant avoir été capable de détecter « 52 % des messages supprimés au second trimestre 2018 » grâce à ses outils de surveillance automatique, contre « 13 % au dernier trimestre 2017 ». En 2018, il y avait soixante

modérateurs. « *On a pu observer une modération plus proactive de Facebook ces derniers mois, mais c'est encore extrêmement partiel et de nombreux messages de haine continuent de circuler. Beaucoup de contenus problématiques datant de 2012-2013 continuent aussi de résider sur la plateforme* ». Les Rohingyas réclament désormais cent trente milliards de dollars de dommages et intérêts à Facebook. Mais « *d'après la loi américaine, Facebook n'a que peu de chances d'être tenu responsable des messages publiés par ses utilisateurs. Pour contourner cet écueil juridique, la plainte des Rohingya met en avant le fait que la loi birmane, qui n'offre aucune protection de ce genre, devrait primer* »[57]. Les lois américaines prédominent donc dans des États instables où des minorités sont menacées.

Au Kenya aussi, en 2022, Meta était poursuivi, par des victimes de cruauté et de harcèlement, à hauteur de 1,5 milliard d'euros pour avoir alimenté la violence ethnique en Éthiopie[58].

Malgré des alertes, Meta semble excessivement peu réactif à entériner efficacement toute violence et ce particulièrement dans les pays du sud, car tous les pays ne semblent pas avoir la même importance pour Meta. « *D'après The Verge[59], Facebook tient une liste à plusieurs niveaux, dans laquelle certains pays présentent plus d'importance que d'autres. Le Brésil, l'Inde et les États-Unis sont au "niveau zéro", qui constitue le niveau de priorité le plus élevé. L'Allemagne, l'Indonésie, l'Iran, Israël et l'Italie sont au "niveau un". Vingt-deux pays appartiennent au "niveau deux" et le reste du monde, placé au "niveau trois", se voit allouer un minimum de ressources. Cela prouve que l'entreprise agit seulement lorsque la pression politique est au maximum et qu'elle y trouve un avantage. Dès lors, des millions d'utilisateurs des pays du Sud se retrouvent sans protection, exposés à des contenus dangereux, extrêmes et haineux, souvent vecteurs de haine et de violence dans le monde réel. Ainsi, en Éthiopie, Facebook n'a pas pris les mesures nécessaires en vue de maîtriser la vague de publications incitant à la violence contre les minorités ethniques. Qui plus est, l'entreprise a connaissance de tous les effets néfastes de ses services sur la vie des populations mais refuse de régler ces problèmes car l'augmentation de ses bénéfices reste sa priorité* »[60].

Que dirait-on si nos médias traditionnels propageaient des incitations à la haine ?

Mais même aux États-Unis, pourtant au niveau de priorité le plus élevé, on constate beaucoup de failles. Ainsi, Katie A. Paul, directrice de Tech Transparency Project[61], s'est créée un profil sur Facebook et s'est inscrite à des groupes de milices et d'extrême droite. Et cela peu de temps après l'invasion du Capitole du 6 janvier 2021. Elle a rapidement reçu des fausses informations, des fausses déclarations sur le « vol des élections » par Joe Biden et… de la publicité pour des équipements militaires. Après recherches sur les raisons de ces recommandations, elle découvre que c'est le mot clé « Milice » qui a inspiré l'algorithme. Or, « *en août 2020, Facebook avait annoncé qu'il avait banni le mot milice et les mouvements extrémistes nationaux de sa plateforme* », révèle Katie Paul[62].

Meta peut prétendre ne pas se mêler de politique, mais il en est un outil privilégié. Meta, Instagram et WhatsApp ont été utilisés pour de la désinformation dans des élections comme celle de Duterte aux Philippines (en utilisant une armée de trolls sur Facebook) ou de Bolsonaro au Brésil (avec des milliers de messages mensongers cryptés circulant sur WhatsApp), au succès de l'extrême droite en Italie, en Espagne ou encore aux USA. Avec Twitter et d'autres, ce ne seront jamais des médias neutres tant qu'ils permettront la propagation de la haine, du mensonge et de la violence. Que dirait-on si nos télévisions, nos journaux ou nos radios propageaient des incitations à la haine, du racisme, des insultes, des arnaques ou des complots ? Pourquoi les lois américaines de liberté d'expression, passent-t-elles outre notre droit national qui exclut l'incitation à la haine, la xénophobie ou encore le négationnisme ? L'État français a démontré qu'il pouvait bannir un Cyril Hanouna de la télévision mais pourrait-il le bannir des réseaux sociaux ? Ce serait visiblement beaucoup plus compliqué.

a. Quand des patrons de la Silicon Valley se droitisent

Elon Musk, fervent défenseur du *free speech* américain, avait racheté Twitter pour une somme pharaonique, particulièrement agacé par les exclusions de comptes, comme celui de Donald Trump, et les filtrages de messages mis en place par le réseau social à la suite de la prise du Capitole. 75 % du personnel est licencié, beaucoup ne toucheront pas leurs indemnités. Lors d'une interview de deux heures qu'il accorde début août 2024, sur son réseau X, à Donald Trump, ce dernier le félicitera pour son courage d'avoir effectué ces licenciements, les deux hommes plaisanteront d'ailleurs sur le fait qu'il « faudrait » pouvoir licencier les grévistes. « *Le syndicat américain des ouvriers de l'industrie automobile (UAW) a par la suite porté plainte devant un tribunal fédéral du travail contre Donald Trump et Elon Musk, accusant les deux milliardaires de "tentative d'intimidation et de menace" envers les travailleurs* »[63].

Après le rachat de Twitter, le nouveau patron parlera même de supprimer les modérateurs de contenus, avant de faire demi-tour. Les employés sont étonnés par l'amateurisme de Musk, qui visiblement s'y connaît beaucoup mieux en vente de voitures électriques qu'en réseau social. Il démontrera même les limites à sa sacro-sainte idée de la liberté d'expression lorsqu'il exclut de

Twitter le compte Elon Jet, qui suit ses déplacements en jet privé, après des menaces contre lui et son fils. Mais aussi des comptes comme ceux des journalistes Drew Harwell, du *Washington Post*, de Ryan Mac, du *New York Times* ou encore de Donie O'Sullivan, de CNN, pour violation des règles de la plateforme de médias sociaux sur la vie privée, avant de faire marche arrière[64].

Et en cette année 2024, il soutient clairement Donald Trump au point d'avoir créé l'America PAC fondé pour soutenir sa campagne pour l'élection présidentielle, avec le soutien d'un certain nombre d'hommes d'affaires de premier plan actifs dans les technologies et gros bailleurs de fonds comme Douglas Leone (milliardaire et figure marquante du monde de la finance et de la technologie), Joe Lonsdale (cofondateur de Palantir Technologies, spécialisée dans l'analyse et la science des données), Tyler Winklevoss (fondateur de Winklevoss Capital Management et de la plateforme d'échange de cryptomonnaie Gemini), Ken Howery (co-fondateur de PayPal), Shaun Maguire de Sequoia Capital (société américaine de capital risque, spécialisée dans l'incubation et le financement d'entreprises innovantes parmi lesquelles Facebook, Apple, Google et YouTube ou encore Oracle)[65], et Antonio Gracias, membre du conseil d'administration de SpaceX. Tous ces noms pour souligner la puissance de feu de cette association avant d'évoquer l'enquête de CNBC sur la suspicion d'utilisation de données personnelles. L'article évoque la collecte d'informations sur les électeurs visant les États pivots[66] via des publicités provocatrices sur Google. Celles-ci mettent en vedette la tentative d'assassinat de Donald Trump, soulignant l'aspect hors de contrôle du pays avant de proposer un lien vers le site de America PAC. Site qui propose de vous aider à vous inscrire pour voter, mais une fois qu'un utilisateur clique sur « S'inscrire pour voter », l'expérience peut être très différente selon l'endroit où il vit… Si c'est un utilisateur d'un État clé, plutôt que d'être redirigés vers la page d'inscription électorale de leur État, ils sont redirigés vers un formulaire d'informations personnelles très détaillé, et y sont invités à saisir leur adresse, leur numéro de téléphone portable et leur âge. S'ils acceptent, le système ne les dirige toujours pas vers une page d'inscription électorale. Au lieu de cela, il leur montre une page de « remerciement ». Quid de cette aide à l'inscription pour voter, proposée ? Au final, elle n'a reçu aucune aide pour s'inscrire mais elle a transmis des données personnelles inestimables à une opération politique[67]. Selon le *Wall Street Journal*, le groupe se serait fixé pour objectif d'inscrire huit cent mille nouveaux électeurs dans les États transitoires pour les élections[68]. Dans une interview de Brendan Fischer, directeur exécutif adjoint de l'ordre de surveillance de la finance de campagne Documented, celui-ci déclare : « *Je pense qu'il est sérieux de supposer que les données des électeurs collectées par ce biais vont alimenter le démarchage de l'Amérique PAC et d'autres activités politiques* ». L'État du Michigan étudie actuellement la question pour voir s'il y a eu violations possibles des lois de l'État[69]. Déjà en mai 2024, Matthew Baum, professeur à la Harvard Kennedy School, dont les recherches incluent l'étude de la désinformation s'inquiétait du phénomène Musk : « *Je dirais qu'il est quelque peu inquiétant que le propriétaire de l'une des plateformes de médias sociaux les plus importantes soit ouvertement partisan et utilise sa plateforme… comme un véhicule pour poursuivre ses objectifs ouvertement partisans* »[70].

Quid de cette aide à l'inscription pour voter ?

Boris Manenti, dans son livre *Elon Musk - Le bonimenteur*, décrypte la lutte d'Elon Musk contre le wokisme via le rachat de Twitter : « *Des positions conservatrices, anti-progrès sociaux, anti-tous genres et le rachat de Twitter c'est vraiment cet objectif-là, de vraiment contrer une certaine idée du progressisme et redonner la parole à l'extrême droite, à des propos transphobes, homophobes, à des propos racistes même* »[71]. Soulignons qu'après le rachat de Twitter, devenu X, le réseau a vu une explosion de messages haineux, racistes et homophobes. Encore une fois c'est le départ de nombreux annonceurs qui fera reculer Musk et tenter de trouver un filtrage. Mais en juillet 2024, malgré ses promesses de les éradiquer, des « bots » diffusent de la désinformation sur l'élection américaine sur X. Et que penser quand Elon Musk partage une vidéo manipulée de Kamala Harris où la candidate démocrate à la présidence américaine déclare que Joe Biden est « sénile » et qu'elle n'a « aucune idée de comment diriger ce pays ». Le patron de X se présente désormais en influenceur politique tout en jouissant d'un grand pouvoir économique, médiatique et désormais politique. Selon un article de RFI, Radio France International, « *Le magnat de la technologie, est de plus en plus influent sur la scène politique américaine. Sa société SpaceX profite de contrats gouvernementaux, et ses véhicules électriques sont très régulés en termes de fiscalité. Elon Musk aurait, selon les observateurs, beaucoup à gagner ou à perdre, en fonction de celui qui occupera la Maison Blanche* »[72].

Et les sorties du milliardaire commencent à sérieusement faire jaser. Août 2024, alors que des émeutes d'extrême droite secouent l'Angleterre, Elon Musk, milliardaire provocateur du secteur de la technologie, affiche sa sympathie pour les manifestants anti-immigration, suscitant la colère du gouvernement britannique, qui accuse les entreprises de médias sociaux d'avoir alimenté l'agitation[73]. D'après un rapport de l'ONG britannique Center for Countering Digital Hate (CCDH) (« Centre contre la haine en ligne »), « *le patron du réseau social X a relayé cette année une cinquantaine d'informations fausses ou trompeuses portant sur la présidentielle américaine à venir. Ses publications ont engendré 1,2 milliard de vues et soulignent une volonté d'interférence toujours plus erratique et aiguisée* »[74]. Le sommet de l'argumentaire complotiste et dé-

lirant est atteint lors du débat télévisé de Donald Trump contre Kamala Harris, où celui-ci a repris à son compte une rumeur provenant de comptes X influents selon laquelle des immigrés haïtiens ont tué et mangé des chats dans la ville de Springfield (Ohio). Malgré l'absence de toute source crédible à cette rumeur, Elon Musk lui a également donné de l'ampleur en partageant un tweet relayant cette fausse information et en ajoutant le commentaire « Votez pour Kamala si vous voulez que ça arrive dans votre quartier ». Son tweet a été vu plus de trente millions de fois[75].

Et que dire quand, à deux semaines de l'élection présidentielle, Elon Musk annonce qu'il donnera un million de dollars chaque jour, par tirage au sort, à un électeur inscrit dans un des sept États-clés, là où se jouait la présidentielle. Mais pour participer au tirage, il fallait signer une pétition conservatrice en faveur de la liberté d'expression et du droit à porter des armes. « *Les Démocrates accusent le milliardaire d'acheter des voix pour Donald Trump. Car si les bénéficiaires sont tirés au sort parmi les signataires de la pétition, ils doivent également être inscrits sur les listes électorales. De quoi alarmer David Becker, un expert en élections, interrogé par CNN : "Il est illégal d'offrir de l'argent ou d'accepter de l'argent ou quoi que ce soit de valeur en échange d'une inscription électorale ou d'un vote. C'était le cas par exemple lorsqu'un glacier a voulu offrir des cornets gratuits à ceux qui venaient avec la preuve de leur vote". Ce sera tout de même long et difficile de prouver que l'offre d'Elon Musk enfreint directement la loi, ce qui lui laisse le champ libre jusqu'à l'élection* »[76].

Et il est loin d'être le seul à soutenir financièrement Donald Trump. Selon le *Financial Time*[77], les investisseurs de la Silicon Valley multiplient les dons en direction de la campagne républicaine et en listait quelques-uns parmi les plus importants, en juillet 2024. La Silicon Valley reste majoritairement pro-démocrate, mais elle n'a pas apprécié certaines volontés de régulations, notamment de l'IA, de l'administration Biden[78]. Même Zuckerberg s'est fendu d'un commentaire contre Biden en exprimant ses « *regrets face aux "pressions" exercées par l'administration Biden en 2021 pour retirer certains contenus liés au Covid-19 de ses plateformes, des critiques saluées par les républicains* »[79].

Quelles peuvent être les conséquences de décisions d'un Elon Musk?

Musk s'était ouvertement plaint d'avoir été peu soutenu par les démocrates pour ses sociétés Tesla et SpaceX[80]. Le colistier de Trump, JD Vance, ancien militaire et investisseur en capital-risque, est également un proche d'un certain Peter Thiel. Ce dernier est cofondateur de PayPal, il « *a employé JD Vance dans sa société de capital-risque, Mithril Capital Management, puis a financé sa campagne au Sénat de l'Ohio avec un don de 10 millions de dollars* »[81] et est, comme Elon Musk, loin de représenter idéologiquement la Silicon Valley. Mais aux yeux des investisseurs et des grandes entreprises, avoir Vance à Washington serait un atout pour la Silicon Valley. Celui-ci est clairement anti-avortement, défend l'idée que les élections de 2020 ont été truquées, il est anti-immigration et ouvertement isolationniste et a fait de X une tribune pour exprimer ses idées ultra-conservatrices. Rappelons qu'il y a notamment répété de fausses rumeurs sur les immigrants haïtiens qui mangeraient des animaux de compagnie à Springfield, dans l'Ohio, et qualifié le Royaume-Uni de « pays islamiste »[82]. Vance suivra-t-il Donald Trump dans ses soutiens aux mouvances suprématistes ou aux complotistes comme QAnon[83] ? Quelles peuvent être les conséquences de décisions unilatérales d'un Elon Musk ? Exemple en juillet 2024, « *Elon Musk a annoncé sur X qu'il allait déplacer au Texas le siège de l'entreprise aérospatiale SpaceX et du réseau social X, afin de protester contre le passage d'une loi sur les élèves transgenres, promulguée en Californie* »[84]. « *"J'ai clairement fait savoir au gouverneur Newsom il y a environ un an que des lois de cette nature forceraient les familles et les entreprises à quitter la Californie pour protéger leurs enfants", écrit-il. L'une des enfants du patron de Tesla a fait son coming out transgenre à 16 ans, et a fait une demande officielle de changement de prénoms en 2021, à 18 ans. Elle a ensuite rompu ses relations avec son père, une décision qu'Elon Musk a attribuée à une éducation scolaire qu'il juge trop progressiste en Californie* »[85]. Par ailleurs, « *Dans beaucoup de ses messages postés sur X, il accuse les démocrates de favoriser l'immigration clandestine, de vouloir restreindre les libertés individuelles et d'endoctriner la jeunesse, des chevaux de bataille de la droite conservatrice américaine* »[86]. L'analyse du CCDH précise que Musk fait même circuler l'idée que les démocrates « importent des électeurs » dans le but d'élargir leur base électorale. Un manque de neutralité évident pour l'homme le plus riche du monde, l'un des plus influents et qui possède un réseau social pour propager ses idées. Rappelons début 2024, X était le septième réseau social le plus utilisé au monde, juste derrière TikTok, avec six cent dix-neuf millions d'utilisateurs actifs[87].

Autre exemple de sa puissance, le 26 février 2022, « *alors que les troupes russes, entrées en Ukraine deux jours plus tôt, menacent de prendre la capitale, Kiev, le ministre ukrainien de la transformation numérique, Mykhaïlo Fedorov, adresse un message désespéré à Elon Musk, propriétaire de l'entreprise spatiale SpaceX. "Pendant que vous essayez de coloniser Mars, la Russie essaie d'occuper l'Ukraine ! (…) Nous vous demandons de fournir à l'Ukraine des stations [de télécommunication par satellite du système] Starlink", supplie le jeune dirigeant sur Twitter. Dix heures plus tard, la réponse du milliardaire américain tombe sur le réseau social : "Le service Starlink est désormais actif en Ukraine. Plus de terminaux sont en route". Près de dix mois après l'attaque des troupes de Vladimir Poutine, les experts*

militaires le reconnaissent : sans l'apport des satellites de télécommunications d'Elon Musk, l'armée ukrainienne n'aurait pas résisté aux assauts russes, en tout cas pas aussi bien ». Musk a ainsi montré qu'il pouvait changer le cours d'une guerre. On lui a d'ailleurs ensuite reproché de ne pas avoir fait la même chose pour Gaza. On peut donc se poser la question des choix, aux conséquences éminemment politiques, d'un Musk.

Autre fait d'un Musk, décidément incontournable dans la conquête de l'espace. À l'été 2024, deux astronautes, Butch Wilmore et Suni Williams, qui ne devaient rester qu'une semaine dans la Station spatiale internationale, ISS, ne rentreront finalement qu'en 2025. En effet, les deux premiers astronautes transportés par le nouveau vaisseau Starliner de Boeing pourraient bien devoir attendre … une capsule de SpaceX pour rentrer sur Terre. Un Musk, déjà partenaire de la NASA pour les missions lunaires et martiennes, est désormais un partenaire privilégié du Pentagone, notamment dans ce qu'on appelle la militarisation de l'espace. Car l'espace est devenu une zone de guerre, au même titre que la mer. Musk devient, au fil des années, incontournable pour la stratégie géopolitique US. Et pendant qu'il détourne l'attention avec une « conquête de Mars » hypothétique, sa société Starlink envoie un nombre astronomique, à vitesse grand V, de satellites en à basse orbite. Les lancements ont commencé en 2019 et six mille sont désormais opérationnels fournissant des services internet dans septante pays[88]. Et la « *technologie d'Elon Musk est déjà utilisée par des entreprises, mais aussi par des agences gouvernementales et des utilisateurs qui ne disposent pas d'une connexion fibre chez eux* »[89]. Beaucoup craignent une situation de monopole dans la distribution d'Internet dans une large partie du monde. Starlink risque de devenir incontournable dans la géopolitique mondiale.

En parallèle, il est courtisé par les dirigeants du monde entier, sans être très regardant sur leurs rapports avec l'état de droit, de la Chine à l'Argentine, en passant par l'Italie, l'Inde ou Israël. Il est reçu avec les attentions accordées habituellement aux chefs d'État, et ses conseils et ses investissements, que ce soit en matière de voitures électriques, d'intelligence artificielle ou de satellite, en font un personnage incontournable sur la scène internationale. Mais le grand défenseur de la liberté d'expression n'a pas fini de se contredire. Lorsque par exemple il accepte de censurer des opposants politiques à la demande du gouvernement turc, à la veille des élections, expliquant que la Turquie avait menacé de bloquer l'ensemble de son réseau social[90]. Ou lorsqu'il censure un lien vers un documentaire de la BBC critiquant le Premier ministre indien[91]. Selon lui la liberté d'expression ne serait pas transposable dans tous les pays, il faut se conformer aux lois d'un pays.

Une parole très relative car, à l'été 2024, dans l'interview précitée qu'il consacre à Donald Trump pendant deux heures sur son réseau social, l'homme aux cent nonante-trois millions d'abonnés, est particulièrement conciliant avec le candidat. La veille, Thierry Breton, commissaire européen en charge de la nouvelle législation sur les services numériques, avait envoyé à Musk une longue mise en garde : « *"Mes services et moi-même serons extrêmement vigilants […] concernant d'éventuelles violations du DSA, et nous n'hésiterons pas à utiliser tous les outils à notre disposition, y compris des mesures temporaires, si cela s'avérait nécessaire pour protéger les citoyens européens" … Le DSA, le Digital Services Act, oblige toutes les plateformes en ligne à mettre en place un système de signalement de contenus problématiques et d'agir "promptement" pour retirer tout contenu illicite ou d'en rendre l'accès impossible dès qu'elles en ont connaissance. Bruxelles a ouvert en décembre 2023 une enquête formelle contre X, soupçonné de manquements à ses obligations en matière de lutte contre la désinformation* ». À cet avertissement, Elon Musk avait alors répondu un message empreint de poésie à l'élu européen : « *Fais un grand pas en arrière et va te faire ***** »[92]. Rappelons que le milliardaire a décidé de suspendre ses opérations au Brésil, à la suite d'un bras de fer avec un juge du Tribunal suprême fédéral, Alexandre de Moraes, qui lui a ordonné de supprimer un certain nombre de comptes disséminant, selon lui, de la désinformation et de la haine en ligne. Volonté, bien sûr, assimilée à de la censure par Elon Musk. Comment faire confiance à un tel personnage qui a, non seulement un pouvoir immense, mais qui se mêle de politique, allant jusqu'à se faire filmer à la frontière, pour donner son avis sur la migration, ou en train de tirer à l'arme lourde ? Pendant qu'il « divertit » les masses, son pouvoir et sa fortune[93] grandissent inexorablement. Un pouvoir du privé qui dépasse celui de certains États. Et il plaît aux partis extrémistes. Ainsi, fin septembre 2024, l'extrême droite européenne, dont fait partie le groupe des Patriotes dirigé par Jordan Bardella, a proposé de remettre le prix Sakharov[94] sur les droits humains au milliardaire Elon Musk. Un candidat choisi pour sa contribution à la « liberté d'expression ».

Ce bras de fer entre un État de droit et un milliardaire de la Silicon Valley est à son paroxysme au Brésil, en cette année 2024. Des soutiens de l'ancien président d'extrême droite, Jair Bolsonaro, opposés au retour au pouvoir de Lula, ont saccagé le Congrès, la Cour suprême et le palais présidentiel à Brasilia, en janvier 2023. Ces attaques contre les institutions démocratiques locales ont été, comme pour l'invasion du Capitole à Washington deux ans plus tôt, encouragées par des discours de désinformations sur les réseaux sociaux. Dans le collimateur du juge Alexandre de Moraes, un des onze membres de la Cour suprême brésilienne et président du Tribunal Supérieur Électoral : le réseau social X, considéré

comme une chambre d'échos aux pires de ces discours. Le bras de fer a commencé quand Alexandre de Moraes a imposé à X de fermer les comptes de sympathisants de l'ex-président brésilien d'extrême droite soupçonnés de diffuser de la désinformation. Elon Musk avait alors dénoncé une tentative de « censure », promis de lever « toutes les restrictions de comptes au Brésil », avant de réclamer carrément la « démission ou la destitution » du juge. On est loin de l'attitude conciliante envers le régime turc d'Erdogan. Le juge a ensuite ordonné des amendes de vingt mille dollars par jour pour chaque compte réactivé, ouvert une enquête pour une présumée « instrumentalisation criminelle » de la plateforme avant de finir par geler les avoirs financiers brésiliens de Starlink, le fournisseur d'accès à Internet par satellite dont Elon Musk est propriétaire, pour récupérer le montant d'amendes non payées par X. Au final, X a été interdit au Brésil. Jorge Messias, l'avocat général de l'Union, chargé de défendre les intérêts du gouvernement Lula, a déclaré « *Nous ne pouvons pas vivre dans une société où des milliardaires qui vivent à l'étranger contrôlent les réseaux sociaux et se montrent disposés à violer l'État de droit, en désobéissant à des ordres judiciaires et en menaçant nos autorités* »[95]. Retenons également cette phrase de Musk, en octobre 2022, après avoir qualifié le juge de Moraes de « honte pour la justice » : « *Ses actions sont incompatibles avec un régime démocratique. Le peuple brésilien doit faire un choix : la démocratie ou Alexandre de Moraes* ». Musk se pose ainsi en garant de la démocratie. Le président Lula avait ensuite réagi sur la radio locale MaisPB : « Pour qui se prend-il ? », « *Tout citoyen de n'importe quelle partie du monde qui a des investissements au Brésil est soumis à la Constitution et aux lois brésiliennes* »[96]. Mais de nombreux partisans de Jair Bolsonaro ont salué l'attitude du milliardaire. Il faut savoir que le pays est très divisé et que le président Lula n'a gagné les présidentielles qu'avec 50,84 % des voix, contre 49,16 % pour Bolsonaro. Elon Musk joue donc un jeu dangereux en soufflant sur des braises déjà bouillantes.

Les réseaux sociaux offrent un ring à la démocratie

Il est ainsi hallucinant de constater qu'un homme puissant se mêle de politique nationale dans divers pays et que son réseau serve de propagande à toutes *infox* ou appels à la haine. Les réseaux sociaux offrent ainsi un ring à la démocratie où se polarisent les camps et les idées, où se disséminent les messages d'agressivité, voire de haine, et où une forme de justice populaire peut détruire des vies. Ils sont encore loin d'être le berceau du débat politique constructif.

Pourrait-on voir X interdit un jour en UE ? Après l'arrestation et la garde à vue, fin août 2024, du patron de Telegram, le réseau crypté du franco-russe Pavel Durov regroupant un milliard d'utilisateurs, le message envoyé aux libertariens du net semble clair : « Vous devez respecter les lois ! ». Durov est en effet auditionné dans le cadre d'une enquête, qui porte sur nombre de « délits de complicité », dont « l'administration d'une plate-forme en ligne pour permettre une transaction illicite en bande organisée », la « détention de l'image d'un mineur présentant un caractère pédopornographique », « escroquerie en bande organisée », « blanchiment » ou encore « escroquerie en bande organisée »[97]. Le bras de fer avec les plateformes semble se durcir entre les pouvoirs publics et des milliardaires qui veulent imposer leur vision de la démocratie.

b. Déplateformisation : solution ou censure ?

Ce terme est assez récent et résulte d'une collaboration éminemment politique entre des États et des plateformes. Lorsque la Russie attaque l'Ukraine, en février 2022, le gouvernement Poutine, à travers des médias sous sa coupe, donne une vision très partiale des événements face à une attaque condamnée par l'ONU. Les deux médias les plus populaires sur les GAFAM, que sont RT (anciennement Russia Today), et Sputnik, seront alors interdits par le Conseil de l'Union européenne, deux mois plus tard. Petit à petit, les GAFAM vont accepter de limiter ces deux médias dans l'UE. C'est ce qu'on appelle la déplateformisation.

À l'évidence, l'UE peut donc pousser les plateformes à faire disparaître des chaînes de propagande et de désinformation et à utiliser les GAFAM comme armes géopolitiques. Mais si RT et Sputnik œuvrent clairement à la déstabilisation des démocraties européennes, notamment en tentant d'influencer des élections comme celles d'Emmanuel Macron en France, ces deux médias se sont aussi rendus populaires en France en soutenant le mouvement des Gilets jaunes. Ce dernier exemple montre la fragilité du principe car il est ouvert à interprétation. Peut-on interdire des soutiens à une révolution populaire ? Dans ce cas, qu'est-ce qui nous permet d'apporter notre soutien à une révolution tunisienne ?

Même provisoire, cette mesure n'est pas sans conséquences. Fermer les canaux d'informations russes est-ce la solution la plus appropriée ? En effet, le gouvernement Poutine a désormais le champ libre pour créer son propre réseau d'information. Rossgram a remplacé Instagram et VKontakte a remplacé Facebook.

Désormais, le peuple russe est enfermé dans un seul discours, celui de l'État.

« *Le contrôle centralisé de ces entreprises sur les flux d'informations mondiaux en fait des acteurs essentiels dans les conflits géopolitiques et les guerres de l'information. On peut même soutenir que ce pouvoir disproportionné qu'exercent les grandes plateformes sur l'espace public numérique arrange les États en temps de guerre, dans la mesure où cela facilite la censure verticale et massive* »[98].

Saisi par RT France, la Cour de justice européenne a tranché : « *Le Tribunal conclut que, compte tenu du contexte extraordinaire de l'affaire, les circonstances suffisent pour établir que les limitations à la liberté d'expression de RT France que les mesures restrictives en cause sont susceptibles de comporter sont proportionnées, en ce qu'elles sont appropriées et nécessaires, aux buts recherchés. Le Tribunal conclut également que lesdites mesures, dès lors qu'elles sont temporaires et réversibles, ne portent pas une atteinte disproportionnée au contenu essentiel de la liberté d'entreprise de RT France* »[99].

4. Privatisation des services publics "grâce" au numérique

Soucieux de se délester de tâches administratives coûteuses et chronophages, nos services publics ont une étonnante confiance envers des entreprises technologiques dont on ne connaît le fonctionnement ni de leurs algorithmes, ni de leurs outils. Nos politiques seraient-ils devenus ingénieurs TIC ? Non, ils sont obligés de se fier à des entreprises, souvent étrangères, pour gérer des problèmes et des données belges, parfois très sensibles.

Et ce n'est pas là un problème purement théorique mais un constat. Prenons l'exemple d'un des leaders de la Tech : Microsoft. Combien d'administrations utilisent des applications appartenant à ce groupe, comme Outlook, OneDrive, LinkedIn ou Exchange ? Un groupe tentaculaire, dont nous avons vu les achats massifs pour une influence toujours plus grande. Elle amasse ainsi toujours plus de données pour alimenter son ogre ChatGPT. Mais peut-on faire confiance à ce partenaire au point de lui laisser accès à la gestion de nos administrations ?

Nos politiques seraient-ils devenus ingénieurs TIC ?

Quelques constats :

- En mars 2021, le Centre pour la Cybersécurité Belgique mettait en garde les entreprises belges contre une attaque des serveurs de Microsoft. Pas moins de mille cent septante entreprises belges risquaient d'être piratées en raison d'une faille de sécurité dans la plateforme de messagerie électronique Exchange de Microsoft, selon Secutec, une société de cybersécurité d'Aartselaar, aux Pays-Bas. Selon elle, des pirates ont réussi à pénétrer dans l'infrastructure informatique d'au moins trente entreprises[100].
- Nous l'avons vu plus haut, LinkedIn, qui appartient à Microsoft, a subi un vol de données de plus d'un demi-milliard de ses utilisateurs, qui ont été extraites de la plateforme et proposées à la vente en ligne. LinkedIn n'a ainsi pu protéger les données de 92 % de ses utilisateurs, dont de nombreux Belges.
- 19 juillet 2024, une panne informatique mondiale chez Microsoft affecte les transports et les télécommunications dans de nombreuses parties du monde. En Belgique, la SNCB, l'aéroport de Charleroi, certaines entreprises ou encore des hôpitaux ont été partiellement bloqués. Une mise à jour déployée par l'entreprise de cybersécurité Crowdstrike a provoqué l'arrêt simultané de plus de huit millions d'ordinateurs sous licence Windows à travers le globe.
- 2023, des hackers ont volé des milliers de comptes ChatGPT (dont Microsoft est propriétaire à 49 %) et les ont revendus sur le *dark web*, exposant les données personnelles et les conversations privées des utilisateurs[101].
- Octobre 2024, des chercheurs, de la firme de cybersécurité Check Point, découvrent plus de cinq mille courriels Microsoft usurpés. Des escrocs se font ainsi passer pour des collaborateurs de Microsoft ou des fournisseurs du géant technologique américain et tentent de tromper les destinataires des courriels. « *Selon la firme de cybersécurité, les messages utilisent des "techniques de dissimulation exceptionnellement sophistiquées", ce qui rend pratiquement impossible pour les utilisateurs de les distinguer des communications légitimes* »[102].
- Octobre 2024 encore Une vaste opération de piratage des bases de données de la police nationale suscite l'émoi aux Pays-Bas – selon la direction de la police, soixante-cinq mille membres des forces de l'ordre seraient concernés. Noms,

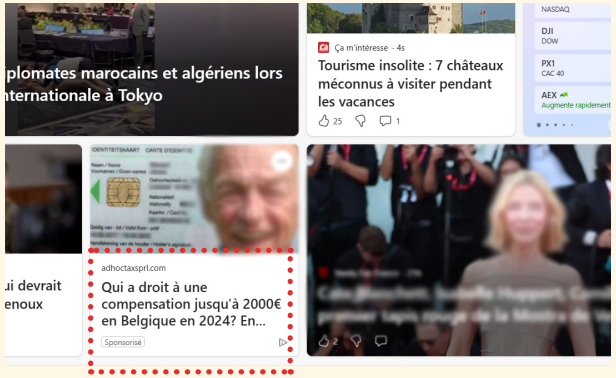
numéros de téléphone professionnels et privés, fonctions exactes, adresses électroniques, contacts, informations sur les enquêtes : ces données auraient été dérobées en utilisant des identifiants Outlook volés à un des policiers, désormais invités par leur hiérarchie à « *une vigilance maximale* »[103].

- Selon le rapport de l'entreprise de sécurité en ligne Check Point Software Technologies Ltd. : « *Pour le deuxième trimestre de 2024, Microsoft est resté la marque la plus imitée dans les attaques de phishing, représentant plus de la moitié de toutes les tentatives avec 57%. Apple a sauté à la deuxième place avec 10 % … et LinkedIn a conservé sa troisième place précédente avec 7% de ces tentatives* »[104]. 57 % des phishings se font donc via Microsoft et « *Le phishing reste l'une des cybermenaces les plus répandues et souvent le point d'entrée d'attaques à plus grande échelle* ».
- Le feuilleton juridique qui fait controverse depuis 2019 en France : Le Health Data Hub (HDH), cette plateforme qui regroupe des données de santé, a pour objectif de faire avancer la recherche médicale. Pour héberger cette infrastructure regroupant les dossiers médicaux des Français, le gouvernement a fait le choix de Microsoft. L'affaire pose pourtant un problème juridique. Les serveurs de Microsoft Azure sont situés en Europe, mais l'entreprise dépend malgré tout de la juridiction américaine. Et notamment de la loi FISA (Foreign Intelligence Surveillance Act), qui autorise la surveillance de masse au nom de la sécurité nationale. Cette loi permet aux agences de renseignement d'accéder aux données de citoyens non américains.

Ces faits nous montrent qu'un État comme la France est tout à fait prêt à confier ses données de santé, parmi le plus sensibles, à un opérateur américain qui peut les partager avec son gouvernement. Et que ce même opérateur peut être victime de vols de données ou d'une panne car, comme l'explique Axel Legay, professeur d'informatique à l'UCLouvain, « *La complexité et l'interconnexion croissante des logiciels nous rendent de plus en plus vulnérables à ce type de pannes* »[105]. Voilà qui n'est pas complètement rassurant.

L'exemple des Pays-Bas est également intéressant car, au-delà des soucis éthiques et techniques des plateformes, des agents de l'État peuvent eux-mêmes être piégés et servir de porte d'accès à des fichiers confidentiels. En l'occurrence avec Outlook, outil de messagerie et d'agenda de Microsoft, très utilisé en Belgique aussi.

Microsoft aurait-il une meilleure maîtrise de ses algorithmes que Meta ? Quand on va sur le moteur de recherche de Microsoft, Bing, il y a des liens vers des médias d'informations, des publicités mais aussi vers de faux articles et des arnaques. Ex : Ci-dessous : Quand on clique sur un article alléchant intitulé « Qui a droit à une compensation jusqu'à 2000 euros en Belgique en 2024 ? » …



On arrive sur un faux site de RTL avec une adresse URL étonnante :

Le genre de faux site qui vous invite évidemment à cliquer sur un lien et à faire un virement, voire à vous demander, a minima, des données personnelles, comme votre numéro de compte.

Microsoft n'est donc pas tellement plus fiable que d'autres GAFAM sur la maîtrise de ses algorithmes.

Mais désormais nos administrations veulent faire confiance à ces entreprises. Pourtant, déjà en 2020, le célèbre politologue américain Francis Fukuyama mettait en garde[106] l'opinion publique contre l'influence politique démesurée qu'ont acquise, en peu de temps, les GAFAM. Surtout après l'expérience Covid-19, où la plupart des solutions pour répondre aux confinements furent numériques. Et, « *Non seulement, les plateformes sont devenues aussi riches que bien des États, mais elles ont acquis un haut degré de contrôle sur la communication politique* »[107]. Comme le soulignait Brice Couturier, sur France Culture : « *Aujourd'hui, l'exigence d'encadrement de ce pouvoir émane principalement des milieux conservateurs qu'énervent les partis-pris progressistes affichés par Jeff Bezos (Amazon), Mark Zuckeberg (Facebook), Sundar Pichai*

(Google) … La Silicon Valley accumule les milliards, mais se donne bonne conscience en proclamant la justice sociale, tendance woke… »[108]. De son côté, Jeff Bezos est loin d'être un ange également. Et s'il manquait d'un réseau social, le fondateur et patron d'Amazon, s'est offert le *Washington Post*, l'un des plus éminents journaux américains. Rappelons l'image très écornée d'Amazon, qu'il s'agisse de son utilisation massive des énergies fossiles, de son management violent et inhumain, de sa recherche de productivité et de performance à tout prix ou de son optimisation fiscale. Fin 2020, trente-sept députés européens, principalement de gauche, dont la Française Leïla Chaibi, attaquaient le géant du e-commerce en écrivant : « *Des signes d'alerte se multiplient sur les politiques antisyndicales et antidémocratiques d'Amazon* ». Ajoutant : « *Jeff Bezos, la liberté d'association, la liberté d'expression et la démocratie ne peuvent être remises en cause par aucune entreprise, y compris la vôtre* »[109]. L'entreprise est en effet connue pour espionner ses employés, et rentabiliser leur travail au maximum, mais aussi les représentants syndicaux, que Bezos ne porte pas en haute estime.

Que ce soit au niveau social, économique, environnemental ou politique, ces nouveaux maîtres du monde bousculent de plus en plus de règles démocratiques. Et ces entreprises investissent désormais massivement dans l'intelligence artificielle, à l'instar des dix milliards de dollars investis par Microsoft dans OpenAI, ce qui risque de décupler leur monopole, tout en accélérant leur puissance algorithmique. En 2024, Alphabet a proposé de racheter Wiz, une start-up spécialisée dans la cybersécurité, notamment dans le cloud, pour la bagatelle de vingt-trois milliards de dollars, mais celle-ci a refusé. Quelles entreprises sont capables d'offrir de telles sommes pour agrandir encore un peu plus leur monopole ? Savez-vous combien vaut Google ? La réponse est mille six cent nonante milliards de dollars en bourse, plus de trois cent milliards de revenus annuels (CA) et septante-quatre milliards de dollars de bénéfices annuels. De quoi faire rêver nos États endettés. Croître, investir, occuper le marché, les GAFAM ne cessent de s'imposer dans toute nouvelle anfractuosité numérique. Une course qui ne laisse pas le temps aux démocraties de résoudre les dommages collatéraux de ces décisions. Politiques, journalistes et experts ne cessent de s'inquiéter du phénomène. En février 2024, des experts en intelligence artificielle, dont des sommités belges[110], et des patrons d'industrie ont signé une lettre ouverte[111] appelant à plus de réglementation autour de la création de ce nouveau phénomène inquiétant que sont les deepfakes, citant les risques potentiels pour la société. En effet, tout va beaucoup trop vite. Demander à nos sociétés de fonctionner aussi rapidement que l'IA est une illusion et une peine perdue. Il faut absolument instaurer des garde-fous. Comme souligné dans notre publication sur les deepfakes[112], ceux-ci concernent souvent l'imagerie sexuelle, la fraude ou la désinformation politique.

5. Hacking, phishing, propagande, harcèlement, arnaques et autres grenades démocratiques

La sécurité est un pilier démocratique. Voilà des siècles que, contre taxes et impôts, les pouvoirs sont censés nous l'assurer. Or, nous subissons un raz-de-marée d'arnaques en tout genre. Rien qu'en 2023, quarante millions d'euros ont été dérobés en Belgique via Internet[113]. Notons ce chiffre étonnant : près d'un tiers des jeunes ne connaissent pas le terme « phishing »[114]. Cette méthode est pourtant massivement utilisée, car les messages sont envoyés par des bots, permettant l'envoi de centaines de milliers d'hameçons, à un prix très démocratique.

Il y a peu, on pouvait encore percevoir quelques fautes d'orthographe, des inepties dans les textes ou une adresse de référence absurde. Exemple avec ce courrier, prétendument envoyé par la Gendarmerie Nationale Française qui nous demande de répondre, à une lettre officielle, sur une adresse Gmail que n'importe qui peut se créer.

Mais désormais, ces messages sont de mieux en mieux réalisés. Aidés par l'IA, les malfaiteurs utilisent des textes bien conçus grâce à ChatGPT, à des imitations de voix bluffantes, à de faux profils, à de faux comptes et même à de fausses images. Une mère peut ainsi entendre la voix de son enfant, par téléphone, la suppliant de lui faire parvenir une somme d'argent.

Ou plus incroyable encore, cet employé d'un centre financier chinois, à Hong Kong, qui a cru participer à une réunion avec des

REPUBLIQUE FRANÇAISE
Liberté – Égalité – Fraternité
MINISTERE DE L'INTERIEUR
Gendarmerie Nationale
BRIGADE DE PROTECTION DES MINEURS

CONVOCATION
N° 7288 BPM

Pour les nécessités d'une enquête judiciaire
(Article 390-1 du Code de procédure pénale)

Nous, Commissaire **Olivier GOUDARD**, Commandant de la Brigade de la Protection des Mineurs (**B.P.M**) en collaboration avec l'Office Européen de Police (**EUROPOL**), vous adressons cette convocation suite à une saisie informatique via cyber-infiltration (autorisée notamment en matière de pédopornographie, pédophilie, cyberpornographie, exhibitionnisme, trafic sexuel, depuis 2014) pour vous informer que vous faites l'objet de plusieurs poursuites judiciaires selon le Code Pénal en vigueur dans le cadre de la Cybercriminalité. Les faits sont les suivants : **PEDOPORNOGRAPHIE – PEDOPHILE – EXHIBITIONISME – CYBERPORNOGRAPHIE – DETOURNEMENT DE MIEURS.**

Notez à titre d'information que la loi de Mars 2007 accentue les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez à cet effet, commis ces infractions citées ci-dessus après avoir été ciblé par notre Cyber-Gendarme grâce à votre flux de données internet, ce qui constitue les preuves de vos infractions.

Vous êtes donc prié de bien vouloir vous faire entendre par email en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions, et cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport au bureau du Procureur adjoint près du Tribunal de Grande Instance de Créteil, spécialiste de la Cybercriminalité afin d'établir un Mandat d'arrêt à votre encontre qui sera transmis à la Gendarmerie la plus proche de votre lieu de résidence. Vous serez donc fiché comme délinquant sexuel et comme l'indique la procédure d'urgence, vos informations seront transmises aux associations de lutte contre la pédophilie et à plusieurs chaînes de télévisions nationales pour une diffusion massive afin que votre famille, vos proches et toute l'EUROPE entière sachent ce que vous faites devant votre ordinateur.

Nous attendons donc vos explications à ces adresses : olivierzgoudard10@gmail.com / olivierzgudard10@gmail.com

Maintenant que vous êtes prévenu, recevez cette Convocation pour servir et valoir ce que de droit.

EUROPOL

Commissaire, Olivier GOUDARD
Commandant de Brigade
Département de la Protection des Mineurs

Direction Générale de la Gendarmerie Nationale - Brigade de Protection des Mineurs
Adresse : 4 rue Claude-Bernard 92130 Issy-les-Moulineaux - Intervention 7j/7j – 24h/24h

cadres supérieurs de l'entreprise alors que tous les participants étaient des « fakes » réalisés grâce à l'intelligence artificielle. Il effectuera pour près de vingt-six millions de dollars de transferts avant de s'apercevoir de la supercherie. Du travail de professionnels.

Ce sont désormais des groupes organisés. Ils s'appellent LockBit 3.0, Babuk Ransomware ou Black Cat et assument totalement leurs méfaits sur le dark web. Un web que les initiés maîtrisent mais pas Monsieur et Madame Tout-le-Monde.

Dans notre étude de 2019, *Fakeland, un nouvel et obscur continent*[115], nous expliquions déjà qu'Internet devenait des sortes d'eaux internationales où sévissaient nombre de pirates en tout genre. Désormais, ils montent en puissance. Ils sont organisés. Ces sociétés ont des développeurs de virus, des employés qui repèrent des cibles via leurs failles informatiques avant de leur voler les données les plus intéressantes, il y a même des « commerciaux » qui négocient le rançonnage des victimes qu'en France les pirates appellent « des viandes ». Des viandes qui sont mangées et qu'ils considèrent comme des idiots, se protégeant mal, car mettant leur prénom ou 1234 en mot de passe. Certains vont jusqu'à dire qu'ils l'ont cherché car ce serait comme laisser la porte d'entrée de sa maison ouverte. Ils se dédouanent de tout, confortablement assis devant leurs écrans, sans aucun contact avec les conséquences de leurs actes et des ravages qu'ils causent[116].

En Allemagne, le fondateur de la Cyberfunk Society, société payée par le gouvernement pour traquer les hackers, explique dans un documentaire[117] ce qui l'a poussé à faire ce métier. Son oncle vendait des objets en ligne. Il a été piraté et les malfrats ont ensuite opéré de fausses ventes en ligne au nom du propriétaire, qui a été tenu pour responsable. Sa vie détruite, il se suicide, endetté à hauteur de 475 000 euros. Les arnaques en ligne et les hackings peuvent ainsi bousiller des vies.

Personne n'est à l'abri, surtout pas de « gros poissons » comme des entreprises dont les lignes de production ont été bloquées à distance. Le patron doit choisir entre payer une rançon ou voir son usine à l'arrêt avec des pertes financières importantes à la clé. Il suffit qu'un seul employé se laisse piéger par un hameçonnage, du style un faux message d'un collègue, et toute l'entreprise en paiera le prix.

Autre exemple les hôpitaux. Des vies y sont en jeu, la vitesse de réactivité y est essentielle et les données contenues dans les fichiers sont particulièrement sensibles. En 2023 c'est le CHRSM de Namur qui a dû se débrouiller pendant des mois avec les vieilles méthodes, avec papiers, bics et imprimantes. En 2022, c'est Vivalia qui est rançonnée. L'intercommunale des soins de santé compte 1472 lits agréés, emploie plus de 3700 personnes et s'adjoint les services d'environ quatre cents médecins spécialisés. Si les choses se sont arrangées, Vivalia n'a jamais voulu dire si la rançon avait été payée.

Autre type de conséquences : le harcèlement. À Tel Aviv, en Israël, en 2021, c'est un site de rencontre LGBT, ATRAV, qui a été rançonné. N'ayant pas voulu payer, les données clients ont été étalées sur le réseau social Telegram. Plusieurs centaines de milliers de messages et de photos privés, en ce compris des nus, des fantasmes secrets et des résultats VIH. Des milliers de personnes ont ainsi été humiliées, dans le pays du judaïsme, qui interdit l'homosexualité[118].

N'importe qui peut aujourd'hui être cyberharcelé et voir sa réputation salie publiquement. Pire, le cyberharcèlement peut toucher nos enfants vingt-quatre heures sur vingt-quatre. « *Une étude commandée par la Secrétaire d'État à l'Egalité des chances Sarah Schlitz (Ecolo) a montré que parmi les filles âgées de 15 à 25 ans, plus de la moitié ont déjà reçu une photo à caractère sexuel (ou "dickpic"), sans y avoir consenti. Il s'agit en général d'une photo d'un pénis, généralement en érection. Selon Catherine van De Heyning (Université d'Anvers), qui a participé à la réalisation de l'étude, les réseaux sociaux doivent assumer davantage de responsabilités, mais il faut aussi travailler à la sensibilisation des jeunes à l'Internet* »[119]. Un tiers des élèves de la FWB serait concerné par le harcèlement, et un « programme-cadre » de prévention du harcèlement et d'amélioration du climat scolaire a été lancé[120]. Il est effectivement difficile de protéger les enfants des messages de

haine, des harcèlements ou encore des images pornographiques, voire pédopornographiques, tout comme des arnaques et des réseaux de propagandes mensongères. La mode depuis peu : les deep nudes dans les écoles. En Belgique, « *une dizaine de jeunes filles de 12 à 16 ans, élèves du collège Saint-Remacle de Stavelot, ont été victimes de deepfakes. Des garçons de leur école et d'autres établissements scolaires ont récupéré les photos qu'elles postaient sur les réseaux sociaux. En utilisant l'intelligence artificielle, ils ont modifié ces photos pour faire apparaître ces adolescentes entièrement nues. Les images ont ensuite été partagées sur Snapchat* »[121]. Une « nouvelle mode » qui tourne parfois au racket, au chantage et/ou au rançonnage.

a. Propagande 3.0

Dans ses tentatives d'ingérence dans les élections américaines ou françaises[122], la Russie reste à la pointe des cyberattaques. Et avec la Chine et l'Iran, elle représente un réseau de propagande puissant, et ce notamment pendant la crise du Covid-19. « *En mars 2020, au moment où l'Organisation mondiale de la santé déclarait une pandémie de COVID-19, le porte-parole du ministère chinois des Affaires étrangères, Zhao Lijian, reprenait sur Twitter une histoire selon laquelle le coronavirus aurait vu le jour aux États-Unis. Cette fausse nouvelle a ensuite été relayée par une myriade de comptes dans plusieurs langues* »[123]. Chine et Russie ont clairement été identifiées comme étant à l'origine de ces fausses informations. « *Nous avons vu une accélération marquée de la mésinformation par des acteurs étatiques, en particulier ceux de la Russie et de la Chine. En fait, 92 % de la mésinformation émanant d'acteurs étatiques proviennent de ces deux pays* »[124], disait Philip Howard, directeur de l'Oxford Internet Institute. Sans parler des réseaux de médias, comme Russia Today ou Sputnik, qui propageaient via Internet de la propagande russe à travers toute l'Europe.

Aujourd'hui, nous « skrollons » sur des réseaux sociaux où se mélangent vraies et fausses informations, ce qui crée une confusion, comme l'a démontré Olivier Klein, professeur de psychologie sociale à l'ULB. Selon son étude, Même une information que l'on sait fausse nous influencera[125].

b. Les élus et autres garants de la démocratie ne sont pas à l'abri

Même les personnalités politiques ne sont pas à l'abri du hacking. En Belgique, des élus ont ainsi été visés par des cyberattaques liées au service de renseignement chinois. Parmi eux, Georges Dallemagne, membre de l'Alliance interparlementaire sur la Chine (Ipac), un groupe d'élus critiques de la Chine : « *Nous n'avons aucune idée de la manière dont cette attaque s'est menée, jusqu'à quel point des données ont été volées et jusqu'à quel point nous sommes encore l'objet de cette attaque et comment nous protéger* »[126], s'inquiète le député Les Engagés.

Au-delà du hacking, les personnalités politiques sont également harcelées. Surtout les femmes. Déjà en 2018, Zakia Khattabi, la co-présidente d'Ecolo à l'époque, annonçait qu'elle arrêtait de communiquer avec les internautes sur Facebook et disait ne pas avoir « *vocation à servir de défouloir et de paillasson à tous les frustrés, fachos, trolls anonymes en tout genre qui sévissent sur les réseaux sociaux* »[127]. La journaliste Florence Hainaut avait alors dénoncé le caractère systématique des insultes et des menaces qui pesaient sur les femmes qui prennent part au débat public : « *Quand on aura enfin compris à quel point ce harcèlement est systémique et n'a d'autre but que de faire taire et invisibiliser les femmes, il sera trop tard* »[128], dénonçait-t-elle. Et l'ex-ministre de la Mobilité et bourgmestre de Jurbise, Jacqueline Galant (MR) d'ajouter : « *Les gens sont d'une violence extrême, Facebook est devenu un déversoir de haine et d'insultes. On reste des humains, on a des familles pour qui ce n'est pas facile et qui en paient le prix* ». En 2019, un autre article dans *La Libre Belgique* : « *Toutes sont attaquées très régulièrement sur les réseaux sociaux, que ce soit par menaces de mort, de viol, des propositions indécentes, des insultes quotidiennes, de drague lourde … L'Institut pour l'égalité des hommes et des femmes a été saisi pour plusieurs cas, mais les victimes n'ont pas pu obtenir justice. En effet, il s'agit souvent de messages privés, or la loi sexisme ne s'applique qu'à la sphère publique* »[129]. Pour faire de la politique sereinement, les messages qui s'attaquent directement à la personne et non à sa politique sont une vraie plaie démocratique.

Et les journalistes, ce quatrième pouvoir, n'est pas épargné. Comme nous le disait en aparté Christophe Giltay, journaliste RTL depuis plus de trente ans : « *Les journalistes sont très bien protégés par la Constitution belge. Aujourd'hui la seule vraie censure que nous subissons est celle des réseaux sociaux* ». En fonction des sujets traités et de la manière dont ils sont traités, les journalistes peuvent être inondés d'insultes ou devenir la cible de groupes de pression[130].

En mars 2019, l'Association flamande des journalistes (VVJ) a mis en place un point de signalement des agressions visant les journalistes. Un article du journal *Médor* de 2021 disait déjà : « *Le harcèlement par la "nouvelle droite", la censure, les messages de haine et les propos diffamatoires sur les réseaux sociaux sont autant de phénomènes en expansion* »[131]… « *En juin 2019, la VRT a mis en lumière les menaces et autres manœuvres d'intimidation de Schild*

& Vrienden, l'organisation de jeunes nationalistes flamands d'ultra-droite. Les techniques de prédilection de ce cercle sont le piratage de comptes personnels (hacking), la divulgation de données à caractère personnel (doxxing) et l'atteinte coordonnée à la réputation ("raid numérique") »[132].

Certaines réactions à l'égard des politiques ou des journalistes sont exacerbées par des propos dénigrants tenus par des personnalités politiques qui éveillent une agressivité chez une partie de leurs sympathisants. « *Les rédacteurs politiques n'échappent pas à cette hostilité croissante dans l'exercice de leur travail. En mars 2019, au nom d'un groupe de collègues, un journaliste de la VRT a dénoncé "l'attitude négative et l'arrogance" des porte-parole politiques. "Quand des correspondants politiques veulent évoquer des affaires pouvant faire apparaître les politiciens sous un mauvais jour, ils sont tout simplement menacés", alerte ainsi la VVJ, qui réunit les journalistes professionnels* »[133].

Peter Verlinden, ex-journaliste à la VRT, a longtemps été intimidé par des représentants du régime de Paul Kagame au Rwanda. En novembre 2019, le ministre de la Justice, Koen Geens (CD&V), a confirmé que des espions rwandais empoisonnaient la vie des opposants au régime Kagame dans notre pays. Des trolls du régime rwandais ont tenté de museler le journaliste expert de l'Afrique en le bombardant sur Twitter. Un journaliste peut donc même subir un cyberharcèlement d'un régime situé à des milliers de kilomètres de chez lui.

Le rapport de la Fédération européenne des journalistes (FEJ) de 2021, signale qu'un nombre croissant de femmes journalistes disent adieu au métier sous l'effet des comportements agressifs et des intimidations en ligne. Une enquête des Nations Unies sur la violence en ligne à leur égard dans le monde affirmait que « *73 % des femmes ayant participé à l'enquête déclarent avoir subi des violences en ligne* », que « *20 % des femmes ayant participé à l'enquête déclarent avoir été attaquées ou agressées hors ligne en relation avec la violence en ligne dont elles avaient été victimes* » et que « *41 % des personnes ayant répondu à l'enquête déclarent avoir été la cible d'attaques en ligne liées, selon elles, à des campagnes de désinformation organisées* »[134].

Même dans des petites manifestations, les journalistes sont régulièrement pris à partie. Martine Simonis, secrétaire générale de l'Association des journalistes professionnels, expliquait, à propos de personnes haineuses envers des journalistes lors d'une manifestation : « *Ce public-là perçoit les journalistes comme des symboles de l'autorité, ce qu'ils ne sont pas : Pour toutes ces personnes en opposition – et c'est tout à fait leur droit de l'être- les journalistes sont les seuls qu'ils peuvent atteindre pour se défouler. Les politiques, ils ne les atteignent pas. Les représentants de l'ordre, ils préfèrent ne pas s'y frotter. Ils assimilent les journalistes au pouvoir… Ce qui est une vraie erreur d'analyse* ». Si Internet n'est pas la cause de ce dernier aspect, il en est une gigantesque caisse de résonance. Méfiance, défiance et défoulements gratuits ont explosé avec lui. Et elle est palpable au quotidien. Lorsque nous donnons des formations sur les médias, nous sommes ainsi fréquemment surpris des opinions à propos des politiques ou des journalistes. Notamment quand, à la question « Qui fait encore confiance à la presse ? », et qu'aucune des dix-huit personnes présentes ne lèvera main. Les mêmes personnes vous citeront des informations fumeuses vues sur Internet comme sûres, une autre parlera du gingembre comme remède au Covid-19 (que les gouvernements nous cacheraient). Dans un autre groupe un participant nous dit que le journalisme est orienté et qu'il y a eu des coups de feu derrière chez lui et que la presse n'en a pas parlé. Nous faisons une vérification et constatons que toute la presse écrite en a parlé. D'ailleurs, dans les différents groupes ainsi rencontrés, rarissimes sont ceux qui lisent un journal. Désormais on s'informe avec les réseaux sociaux, où se mêlent opinions, infox et notifications et il est de bon ton de dénigrer les journalistes sans faire la part des choses. Pour Yves Collard, formateur chez Média Animation[135] et spécialiste des complotismes, il s'agit surtout de réactions « antisystème », de défiances envers une société à laquelle beaucoup ne croient plus. Et cette défiance serait fortement accentuée par Internet.

Un logiciel qui permettait de prendre le contrôle d'un smartphone à distance

Par ailleurs, le cas de Pegasus fait froid dans le dos. L'entreprise israélienne NSO, prétendait ne vendre son logiciel espion qu'exclusivement à des clients gouvernementaux, ne collectant que les données provenant des appareils mobiles de personnes soupçonnées d'être impliquées dans des activités criminelles graves et terroristes. Un logiciel qui permettait de prendre le contrôle d'un smartphone à distance sans nécessiter la moindre manipulation de l'utilisateur. Une fois installé, Pegasus donnait un accès total au téléphone, y compris aux messageries cryptées, et permettait même d'activer à distance le microphone et la caméra de l'appareil. En 2021, une fuite de cinquante mille numéros de téléphone a révélé que cent quatre-vingts journalistes avaient été ciblés, avec ce logiciel, dans le monde, particulièrement en Inde, au Mexique, au Maroc, mais aussi en l'Arabie saoudite, aux Émirats arabes unis, au Kazakhstan, en l'Azerbaïdjan, au Togo, au Rwanda, et même en Hongrie, un membre de l'Union européenne. Des agences gouvernementales ciblent leurs propres concitoyens, ainsi que des personnalités à l'extérieur de leurs pays, qui n'ont pour seul tort que d'être avocats, journalistes, diplomates, médecins, sportifs, syndicalistes, simples militants, ou hommes-femmes politiques,

y compris des ministres, et treize chefs d'État ou de gouvernement[136]. On parle donc ici, d'une société privée, opérant depuis un État démocratique, qui vend un logiciel extrêmement intrusif, à des États connus pour leur politique répressive en matière de droits de l'Homme et contre des journalistes. En France, où les autorités n'étaient en rien responsable, près de mille personnes faisaient partie de la liste dont de nombreux journalistes.

Nous ne reviendrons pas sur l'opportunité exceptionnelle qu'ont représenté les réseaux sociaux pour les partis extrémistes, muselés jusque-là par les médias et les partis dits « classiques ». Ils ont su utiliser ce nouvel outil pour optimiser la propagation de leur discours de haine, comme Hitler avait su profiter de nouveaux systèmes de son permettant de porter sa voix devant une foule de près de deux cent mille personnes. Le VlaamsBelang en Flandre a ainsi attiré nombre de jeunes avec de fausses informations sur la migration, les Wallons, l'Europe, les gauchistes… Comme souligné dans notre étude sur les fake news, nombre de partis d'extrême droite ont utilisé ces médias 'de proximité' apparente que sont les réseaux sociaux à travers le monde et l'Europe. François Debras, professeur associé à l'ULiège et spécialiste des discours de l'extrême droite souligne un autre aspect, celui d'une information abrégée, fonctionnant exclusivement par extraits choisis : « *L'information est raccourcie pour être plus accessible. C'est plus facile de tomber dans le populisme. La haine se propage aussi beaucoup plus rapidement que les autres sentiments* ». Et on en revient toujours là. Les réponses faciles aux problèmes complexes et l'émotionnel ont pris le pas sur la nuance et le rationnel. Il est ainsi clair qu'Internet a accentué un ras-le-bol général de citoyens qui ne se retrouvent pas dans une économie mondialisée, mais en se désinformant.

Et cette défiance envers nos élus pourrait être accentuée par l'explosion des hackings et des arnaques en lignes. Car tout ce qui est connecté est théoriquement piratable, comme les appareils de domotique ou les caméras de surveillance de son domicile. Des caméras censées protéger votre maison et qui se retournent contre vous, se transformant en espions capables de voir si quelqu'un est présent sur les lieux et/ou repérer les habitudes des propriétaires, voire des images compromettantes. Il a été démontré que même des voitures autonomes pouvaient être piratées. Alors aujourd'hui une nouvelle question se pose : nos institutions peuvent-elles nous protéger ?

c. Nos institutions peuvent-elles nous protéger ?

Tant bien que mal, les pouvoirs publics tentent de pallier cette épidémie de cybercriminalité. Mais en ont-ils les moyens ?

Déjà, en 2018, le réseau de données de l'État allemand, et de plusieurs ministères, aurait été infiltré sur une longue période par des hackers russes[137].

Côté belge, on n'est pas en reste. Juin 2021, une cyberattaque d'envergure avait touché mille huit cents ordinateurs de l'administration communale de Liège, au point de perturber et ralentir toute une série de services de la Ville[138]. La même année, le village de Floreffe est piratée par un hacker, mais heureusement les données de la commune sont cryptées et inutilisables. Il y aura également la commune de Willebroeck et même la Défense belge, victime d'une attaque sur ses serveurs fin 2021. Elle a dû lancer son « Cyber Command », cinquième composante de la Défense, après l'air, la terre, la marine et le médical[139].

Août 2022 : « *Le groupe de hackers LockBit 3.0 réclame 200.000 $ à la commune de Maldegem, en Flandre-Orientale. Les pirates affirment avoir fait main basse sur des données sensibles et confidentielles, venant en droite ligne du CPAS notamment* »[140].

Tout cela n'a pas empêché de constater, durant l'année 2023, que des sites internet d'institutions belges (comme ceux du Palais Royal, de la Chancellerie du Premier ministre et du Sénat) ont connu quelques perturbations, résultat d'un cyberattaque DDoS[141], qui visait les sites web des services publics belges. Des attaques qui se sont répétées. Difficile de retrouver les auteurs mais « *le groupe de hackers prorusse "Noname" aurait annoncé une attaque de ce type en critiquant l'aide apportée par la Belgique à l'Ukraine, notamment à la suite de l'annonce d'envoi d'avions militaires F-16* »[142], selon Katrien Eggers, porte-parole du Centre pour la cybersécurité Belgique (CCB). Nous l'avons vu, lors de l'attaque de l'Ukraine, la Russie a les moyens de bloquer des institutions publiques et ne s'en cache pas.

Et il ne s'agit là que de nos grandes institutions fédérales. Que dire des administrations communales. Ont-elles les moyens de se prémunir de telles attaques ?

En 2023, c'est tout le CPAS de Charleroi qui était hacké et bloqué pendant des mois. Tous les employés qui n'avaient pas fait de backups ou de retranscriptions écrites, se sont retrouvés totalement démunis. Selon une source non officielle, rencontrée sur place, il se serait également agi d'une attaque russe. Mais ce qui nous a particulièrement marqué c'est que les hackeurs auraient eu accès à des dossiers de réfugiés ukrainiens, que nos institutions sont censées protéger.

Et à nouveau, en octobre 2024, une nouvelle cyberattaque contre les sites de plusieurs communes belges a lieu. Le collectif de pirates informatiques pro-russes, NoName057, est encore à l'origine de l'attaque. Les communes d'Enghien, Comines-Warneton, Mouscron, Flobecq, Amblève, Colfontaine et Malmedy sont notamment touchées pendant plusieurs jours, pour certaines[143].

Il y a clairement un manque de prise au sérieux du problème, notamment dans les moyens mis en œuvre. La course au numérique serait-elle plus importante que la sécurité de nos données ? Il semble évident que les bœufs sont placés avant la charrue. Comment nos autorités communales, nos écoles ou nos lieux culturels peuvent-ils rivaliser avec des hackers professionnels, avec des moyens importants et du matériel de pointe ? Il faudrait donc investir pour se protéger et former. Avec, bien sûr des moyens publics. Or les Régions bruxelloise et wallonne comme de nombreuses communes belges, sont déjà endettées. La question principale n'est-elle pas la suivante : la numérisation de nos communes fait-elle gagner autant d'argent que cela au final ? En effet, investir dans le numérique implique investir aussi dans la sécurité. Et comme on l'a vu, les investissements sont indispensables et onéreux, sans compter qu'ils se font sur le personnel qui n'est plus engagé et les citoyens qui n'ont plus d'interlocuteur.

La transition numérique est donc synonyme de dégradation administrative

De son côté, la Commission européenne ambitionne que, d'ici 2030, la totalité des services publics et des démarches administratives (y compris la santé, les banques et la carte d'identité) devront être numérisés. Du coup l'ex-ministre bruxellois de la Transition numérique, Bernard Clerfayt, tente de faire passer une ordonnance pour numériser les services publics bruxellois contre l'avis de plus de deux cents ASBL travaillant dans l'associatif, dont Citoyenneté & Participation, non seulement parce que cette ordonnance ne garantit pas clairement le maintien de guichets, avec un être humain à qui parler, mais également parce que ces associations doivent accueillir des milliers de personnes perdues quand elles doivent, ne fût-ce que prendre un rendez-vous à la commune et qu'au téléphone on les renvoie systématiquement vers le site internet. Comme le soulignait Elise Degrave, qui travaille au Centre de recherche information, droit et société (CRIDS) de l'Université de Namur : « *C'est la première fois en Belgique que des citoyens manifestent contre la numérisation de la société. Ça montre à quel point il s'agit d'une question démocratique* »[144].

Pourtant le 12 janvier 2024, l'Ordonnance numérique est adoptée, sur le fil, par quarante-cinq voix de parlementaires bruxellois sur quatre-vingt-neuf.

Dans un article du journal *Le Soir*, publié en février 2024, Anne-Emmanuelle Bourgaux, professeure de droit constitutionnel, UMONS et ULB, s'en prenait à cette ordonnance : « *Selon le rapport de la Fondation Roi Baudouin de 2022 sur l'inclusion numérique, la fracture numérique n'est pas seulement générationnelle. Elle est aussi sociale et genrée. Près d'un ménage sur cinq à faibles revenus ne dispose pas de connexion internet à la maison. Plus de la moitié des administrés à faible revenu et à faible scolarité n'utilise jamais l'e-administration. Les femmes sont les plus fragiles face aux compétences numériques. Les services en ligne profitent essentiellement aux utilisateurs multi-connectés possédant de bonnes aptitudes technologiques, soit ceux qui détiennent plus de revenus et plus de diplômes* ». Et d'ajouter : « *Cédant à une modernité mal comprise, la Région bruxelloise est en retard. En France, le Défenseur des droits dénonce dès 2022 que la digitalisation des services publics transfère le poids de la charge, des erreurs et des dysfonctionnements techniques sur les épaules des administrés et des travailleurs sociaux. La transition numérique est donc synonyme de dégradation administrative pour tous les administrés, pas seulement des plus fragiles* ». Soulignons par ailleurs que la Belgique a des services télécom plus chers que ses cinq voisins depuis des années[145]. Ce qui va nettement à l'encontre des volontés de numérisation des Belges.

Concernant les décisions pour la digitalisation de l'administration, Elise Degrave ajoute : « *On entend souvent dire que le numérique est une affaire de technique ; les politiques eux-mêmes la délèguent à des consultants "pour ne pas rater le train de la modernisation" de l'administration. Dans les cabinets, y compris celui du ministre de la Transition numérique, il arrive que des collaborateurs émanent de l'univers de la consultance et du management, là où le numérique a tendance à être considéré comme une fin en soi. … Et comme la numérisation des services publics est entre les mains de techniciens et de consultants qui vendent leur outil, il y a un réel déficit démocratique, d'autant plus qu'on ignore qui sont les concepteurs* »[146].

Pour les autorités, les citoyens n'ont qu'à suivre le train du numérique, qui s'avère être un TGV, et apprendre en allant dans des Espaces Publics Numériques ou en trouvant des séances d'éducation aux médias. Est-ce ça aujourd'hui un service au public ? Faire remplir des formulaires complexes au citoyen, au risque qu'il commette une erreur et se voit refuser une allocation à laquelle il a pourtant droit ? D'autant que, comme le dénoncent depuis des années les services de simplifications administratives, les sites sont trop complexes. À ce sujet Elise Degrave précise : « *C'est l'État qui devrait mettre en place un outil qu'on peut utiliser facilement, et non la personne qui doit compenser le fait que l'outil n'est pas au point* ». Dans notre démocratie, des centaines de milliers de personnes risquent de perdre leurs droits d'accès à un service

dit public. D'autant que peuvent alors se poser de nouveaux problèmes, comme :

- pour faire évoluer leurs algorithmes, les logiciels utilisés par les pouvoirs publics risquent de n'avoir de retour que des personnes utilisant les nouvelles technologies. Et peu celles des gens aux bas revenus et/ou des personnes âgées, premières victimes de la fracture numérique ;
- comme souligné dans l'analyse d'Edgar Gillet, *Numérisation du recrutement et de l'orientation*[147], il faudra passer par des logiciels, souvent programmés à l'étranger par des personnes qualifiées, donc majoritairement issues de classes moyennes, voire aisées, souvent blanches et mâles, ne connaissant pas les spécificités locales, et donc reproduisant des inégalités dans leur programmation, comme le machisme ou le racisme ;
- quid des problèmes matériels rencontrés par certaines personnes ? Au-delà d'avoir un ordi, une imprimante, un scanner et un lecteur de carte, ils doivent être à jour technologiquement. Lors d'une formation, un monsieur nous expliquait que sa banque lui avait fait acheter un nouvel ordinateur car le sien n'était pas compatible avec le PC banking. Il semble que l'e-administration risque de suivre cette trace dans le but de faire évoluer la sécurité en ligne ;
- les citoyens ont l'obligation de veiller à la mise à jour de leurs logiciels et de leurs mots de passe, ce qui n'est pas une évidence pour beaucoup ;
- quelles garanties de sécurité offrent les services publics contre des arnaques boostées à l'IA (faux courriers administratifs, fausses vidéos du bourgmestre, fausses photos, fausses voix, faux profils…) ?

Le hacking peut avoir des conséquences pour les citoyens, que les politiques ne semblent pas percevoir. Prenons un cas concret, et même s'il se passe en Suisse, il est fort représentatif du décalage entre les politiques et les possibilités de piratage. En 2021, à Rolle, un petit village de 5300 habitants, l'administration communale est hackée. Les autorités locales refusent de payer. Deux mois plus tard, un habitant découvre que ses données personnelles circulent sur le web. Car si on ne paie pas, les malfrats se font de l'argent en revendant les datas, ou se vengent en les mettant en ligne. Cela a fait scandale dans la région, car les autorités ont cru qu'elles géraient et n'ont pas prévenu les habitants[148]. Résultat, des données sensibles des habitants comme leur adresse, numéro de registre national, copies de cartes de crédit, signature et des copies de leur carte d'identité ont été divulguées. Sachant que ces deux dernières données peuvent permettre d'ouvrir un compte en banque en ligne, ce vol est gagnant à tout point de vue. Et ces actes ont été revendiqués par Ransomware Vice Society, considéré comme russophone et pas du tout inquiété pour ses méfaits. Mais il ne faut pas spécialement être russe ou sorti de hautes écoles. En 2024, Julius Kivimäki a été condamné à six ans et trois mois de prison, pour avoir fait chanter trente-trois mille personnes en menaçant de publier en ligne les notes de leurs séances de thérapie. Le « business » de ce jeune finlandais a duré onze ans et a « *commencé lorsqu'il a acquis une certaine notoriété au sein d'un réseau anarchiste de pirates informatiques adolescents, alors qu'il n'avait que 13 ans* »[149]. Il était devenu l'un des criminels les plus recherchés d'Europe. Il avait déjà été arrêté à l'âge de dix-sept ans, en 2014, puis relâché. À l'époque il avait été reconnu coupable de … 50 700 cas de piratage informatique[150]. Il n'a jamais révélé le montant de son portefeuille, en bitcoins bien sûr.

Autre exemple inquiétant, en 2021, une attaque informatique a visé à empoisonner l'eau distribuée à quinze mille résidents d'une ville de Floride, Oldsmar, elle a été déjouée *in extremis*. Le traitement de l'eau, géré de manière informatique, a été piraté en quelques minutes avant que le taux d'hydroxyde de sodium – soude caustique – ne soit augmenté et déversé dans les eaux[151]. Heureusement un employé s'en est rapidement aperçu avant d'intervenir. Fin 2023, les autorités fédérales américaines annonçaient que près de dix compagnies des eaux aux États-Unis avaient été piratées, heureusement sans conséquences[152]. Ces dernières attaques semblent avoir été menées par des Iraniens, sur des logiciels israéliens utilisés par ces compagnies. Quand la géopolitique s'invite dans la distribution d'eau de petites villes américaines !

Les États et les hackers sont partis pour un long jeu du chat et de la souris

La cybersécurité doit donc être pensée jusque dans les moindres détails, par l'administration et les entreprises. Vouloir tout connecter, pourquoi pas, mais en sachant que tout objet connecté peut être piratable et que les employés peuvent être hameçonnés.

En Belgique, des méthodes de lutte efficaces se mettent en place. Mais le phénomène est tel que l'État a décidé, début 2023, que les « *hackers dits "éthiques" – c'est-à-dire ceux qui piratent des plateformes sans intention de nuire – vont pouvoir bénéficier d'une protection juridique si leurs actions répondent à un certain nombre de critères, a annoncé le Centre pour la Cybersécurité Belgique (CCB)* »[153]. Cela veut donc dire que les États et les hackers sont partis pour un long jeu du chat et de la souris, boosté par l'IA.

De son côté, « *l'Union européenne envisage de nouvelles mesures de cyberdéfense, notamment le recours au "hacking de représailles"* » en réponse à l'augmentation des cybermenaces. Le plan d'action, soutenu par le Forum cybernétique transatlantique inclut des mesures agressives telles que le piratage ou la désactivation d'infrastructures ennemies. D'autres pays comme l'Australie,

le Japon, la Chine et les États-Unis ont également adopté des politiques similaires. Le plan d'action suggère des opérations telles que le blocage de trafic malveillant et la neutralisation de logiciels malveillants. Cependant, les risques de dommages collatéraux et d'escalades diplomatiques demeurent des préoccupations majeures[154]. Des autorités locales, via Internet, peuvent ainsi se retrouver embarquées dans une cyberguerre latente internationale et dans une vague de cybercriminalité.

Selon les statistiques de la police judiciaire allemande, le taux d'élucidation des affaires de cybercriminalité est de 30 %, plus bas que tout autre crime ou délit. Car les poursuites judiciaires sont difficiles. Et puis, il est très complexe d'en venir totalement à bout, les logiciels malveillants étant majoritairement à l'étranger. Exemple avec Emotet, redoutable logiciel malveillant de type « cheval de Troie » qui a infecté 1,6 million d'ordinateurs dans le monde. Le 27 janvier 2021, Europol a annoncé avoir neutralisé le réseau (botnet) servant à la diffusion d'Emotet. Mais après dix mois d'inactivité, une nouvelle version d'Emotet aurait été identifiée. Le CERT-FR[155] a observé une recrudescence des attaques, notamment en France, dès le mois de juillet 2021[156].

Petit à petit des structures se mettent en place. Mais combien de données ont-elles déjà été volées ? De quelle manière vont-elles être utilisées ? Et la totalité des administrations pourra-t-elle garantir la sécurité des données de ses citoyens ? Difficile de donner une réponse.

d. Utilisation des datas par les autorités, la tentation

Au-delà de l'utilisation des datas par des personnes malveillantes, la question de leur utilisation par nos pouvoirs publics fait également débat.

Les traces numériques que nous laissons peuvent tout d'abord nous trahir et ce, même dans une démocratie, en cas de changement de régime politique ou de loi. Exemple aux USA, la Cour suprême permet à chaque État américain qui le souhaite d'interdire l'avortement, depuis 2022. « *Celles et ceux qui cherchent, offrent ou facilitent l'accès à l'avortement doivent, désormais, partir du principe que toutes les données qu'ils et elles laissent sur Internet ou ailleurs peuvent être recherchées par les autorités* ». Le communiqué de l'Electronic Frontier Foundation, principale organisation de défense des libertés numériques aux États-Unis, a énoncé le défi qui se pose à l'industrie technologique … « *L'historique des requêtes Google, par exemple, peut être utilisé par la justice pour renforcer un dossier ou appuyer une inculpation. Si une personne fait une recherche sur des cliniques dans un État voisin disposant d'une législation différente, ou sur les pilules nécessaires à un avortement médicamenteux, ces données peuvent être obtenues par la justice, aussi bien via la saisie des téléphones et ordinateurs, que via une demande au moteur de recherche concerné* »[157]. Nos datas peuvent ainsi se retourner contre nous.

Et que dire de l'utilisation des algorithmes d'aide à la décision dans le cas de justice prédictive. Aux États-Unis, de nombreuses juridictions locales utilisent des logiciels prédictifs pour tenter d'évaluer les risques de récidive des prévenus. Une enquête de ProPublica, publiée en 2016 montre que ces algorithmes sont peu efficaces[158]. Et les résultats sont accablants : le score reflète de manière incroyablement erronée le risque de commission d'un crime violent : seules 20 % des personnes dont le programme estimait qu'elles commettraient un crime violent l'ont fait… Autre sujet d'inquiétude, le logiciel surpondère systématiquement le risque de récidive pour les Afro-Américains, qui se voient deux fois plus souvent que les Blancs attribuer un risque de récidive moyen ou important, notent les auteurs de l'étude. Surtout, le programme échoue dans les deux cas : il surévalue largement le risque de récidive des Noirs et sous-estime ce risque pour les Blancs, montre l'analyse des condamnations ayant eu lieu par la suite. Interrogé par ProPublica, Mark Boessenecker, un juge du comté de Napa (Californie), qui a utilisé le logiciel, estime que c'est, dans son ensemble, la méthodologie des logiciels prédictifs qui est biaisée : « *Un type qui violente un enfant tous les jours pendant un an obtiendra peut-être un score de risque faible parce qu'il a un boulot. Alors qu'un type arrêté pour ivresse publique obtiendra un score élevé parce qu'il est sans domicile fixe. Les facteurs de risque ne vous disent pas si une personne doit aller en prison ; ils vous disent surtout quels sont les bons critères fixer pour une mise à l'épreuve* »[159]. Encore une fois, l'opacité de leur programmation pose un réel souci.

Des techno-solutionnistes de tout poil tentent ainsi de nous vendre l'algorithme comme la panacée à tous nos problèmes, un outil magique, comme s'il n'y avait pas de possibilités d'erreurs, de programmations biaisées ou d'interprétations hasardeuses. Et on en a remis une couche avec l'IA, que certains prennent carrément pour une nouvelle pythie. Or l'IA n'est rien de plus qu'un super calculateur, il gère des statistiques à la vitesse de l'éclair mais il peut générer ce qu'on appelle des hallucinations, c'est-à-dire qu'il invente des infos ou en biaise. Prenons cet exemple d'un cabinet d'avocat New-Yorkais qui a invoqué six arrêts, renvoyant à de

fausses décisions de justice et mentionnant de fausses citations. Ils ont avoué avoir trop fait confiance à ChatGPT[160].

Côté belge, la grosse enquête du *Soir* sur le traitement de nos datas est saisissante. Cette enquête de longue haleine réalisée début 2021, en pleine crise Covid-19, est impossible à résumer en quelques lignes. Nous nous contenterons de souligner la conclusion de Philippe Laloux, spécialiste des questions numériques au journal *Le Soir*. Elle est sans équivoque : « *On y découvre, en vrac, un ovni institutionnel, le Comité de sécurité de l'information (CSI) qui s'est substitué au Parlement pour autoriser les administrations à traiter nos données, en dehors des radars du Conseil d'État et de l'Autorité de protection des données (APD). On aperçoit un chien de garde de la vie privée, l'APD, qui aurait oublié de mordre les autorités. Tétanisé par de sérieux conflits d'intérêts (mettant en péril sa sacro-sainte indépendance), il est aussi "bypassé" par le CSI ou les autorités flamandes qui ne le consultent plus. Dans la salle des machines, on retrouve la Smals, véritable "filiale informatique" de l'État à qui l'on confie, sans marchés publics transparents, les bases de données centralisées ou les algorithmes de traitement de nos données* »[161].

Le numérique est surtout une question démocratique

Il semble que, quand on parle d'Internet, beaucoup ont du mal à prendre les choses autant au sérieux que dans la vie réelle. Depuis 2007, Elise Degrave questionne l'usage du numérique au regard des lois. Elle s'inquiète d'une certaine légèreté et d'une opacité avec laquelle les questions numériques sont traitées par les autorités, notamment au niveau de l'utilisation de nos données, au risque de tomber dans une société de la surveillance et de l'exclusion, menaçant nos droits et libertés humaines garantis par la Constitution, tels que le droit de circuler, de se rassembler, du respect à la vie privée. « *On fait passer le numérique pour une question technique. Or, le numérique est surtout une question démocratique vu l'impact qu'il a à tous les niveaux de la vie des citoyens. Dans la loi "pandémie", il était initialement prévu la possibilité de rassembler, en cas de crise sanitaire, toutes nos données et de les utiliser dans un but de surveillance intensive. Cette disposition a été supprimée après mon audition au parlement. J'essaie ainsi de jouer un rôle de lanceuse d'alerte* »[162]. « *Les algorithmes ne tombent pas du ciel. Ce sont des formules mathématiques conçues par des humains. A la différence des lois, les algorithmes des services publics sont élaborés sans débat démocratique, ni transparence, ni publication, ni même de recours possible. Or, ils sont porteurs de choix politiques et certains peuvent entraîner des effets discriminatoires* »[163]. Elle donne même un exemple assez inquiétant : « *Un ministre wallon a d'ailleurs fait circuler un projet de loi censé permettre de transférer les données de santé des Belges aux sociétés d'assurance, soi-disant pour des motifs d'efficacité - il y a toujours une bonne raison a priori. Mais en creusant, on voit pointer le problème : si ce projet de loi était passé, les assurances auraient pu adapter les primes en fonction de l'état de santé de leurs clients. Le projet a été enterré, mais il pourrait ressortir.* »

En Europe, même si la Commission intime aux États de numériser leurs services publics, elle est malgré tout assez attentive au problème des données personnelles. Deux textes régissent les datas en UE : le Règlement général sur la protection des données (le RGPD), qui garantit la protection des données personnelles des Européens, et, pour les réguler, un « *triptyque :*

- *le "Data Act"*[164] *ou règlement européen sur les données, entré en vigueur le 11 janvier 2024, qui définit des droits d'accès à des données du secteur privé,*
- *le "Data Governance Act", qui va définir les mécanismes, la structure et les acteurs du partage des données, dans ce nouveau marché européen de la donnée. Ces data vont permettre de nourrir les systèmes d'IA, d'où :*
  - *l'AI Act (le Règlement sur l'intelligence artificielle), en cours depuis le 1er août 2024, qui régule l'utilisation des datas par l'IA, oblige à indiquer clairement aux utilisateurs qu'ils interagissent avec une machine, à veiller à ce que certains contenus générés par l'IA doivent être signalés comme tels, à ce que les logiciels médicaux fondés sur l'IA ou les systèmes d'IA utilisés pour le recrutement ou encore les systèmes d'IA qui permettent une "notation sociale" par les gouvernements ou les entreprises.*

Avec ces trois nouveaux textes, l'Union européenne (UE) cherche à atteindre deux objectifs contradictoires. D'un côté, elle souhaite mettre en place un cadre d'exploitation et de partage des données qui soit respectueux des valeurs et de la réglementation européenne. De l'autre, il s'agit de créer un écosystème qui permette aux données de circuler le plus possible. Dans ce système, les data doivent pouvoir être exploitées en masse, on doit pouvoir croiser des milliards de données pour développer des technologies d'intelligence artificielle »[165].

Ce sera le défi à venir pour toutes les démocraties. Faire circuler nos données mais pourront-elles le faire en garantissant leur sécurité absolue ? Ce qui est sûr c'est que ces datas seront convoitées par de nombreux hackers, qu'ils travaillent pour eux-mêmes ou pour un client.

Il faudra également faire respecter les nouvelles réglementations aux géants des plateformes. Rappelons que rien que pour Google, la Commission Européenne a infligé, en 2017, une amende de 2,42 milliards d'euros, suivie d'une amende de 4,34 milliards en 2018 et de 1,49 milliard en 2019, pour position dominante, via son système Androïd. Combien d'entreprises auraient résisté à des telles

amendes sans changer immédiatement leurs positions ? Le bras de fer va sans doute continuer mais subsistent encore des questions sur la récolte des données des citoyens via les multiples applications utilisant l'IA et dont les arcanes du fonctionnement restent quelque peu mystérieuses. Personne ne peut affirmer aujourd'hui que ces IA ne sont pas piratables. Des IA construites, elles-mêmes, sur base de vols de données. Rappelons que le *New York Times* a porté plainte auprès d'un tribunal fédéral à New York, à l'encontre d'OpenAI, créateur du logiciel ChatGPT, ainsi que de Microsoft, son principal investisseur, pour violation des droits d'auteur. Selon le NYT, ChatGPT « *repose sur des modèles d'apprentissage massif construits en copiant et en utilisant des millions d'articles du Times protégés par les droits d'auteur* »[166]. Un phénomène dénoncé par de nombreux artistes, traducteurs ou écrivains. Même notre voix et notre image sont aujourd'hui duplicables par l'IA, pourtant nous en sommes clairement le propriétaire.

Nous nous ruons donc sur une intelligence artificielle qui va bouleverser le monde sur base… du vol de milliards de données par les GAFAM et autres BATX.

6. La fracture sociale numérique, un frein aux espoirs de démocratie numérique

Au départ, Internet a été vu comme un espoir de reprise de contact avec le citoyen et de démocratie participative. On pense bien sûr au modèle estonien. Sa sécurité numérique s'est d'ailleurs faite à l'épreuve du feu, après des attaques massives de la Russie en 2007, suite à un conflit diplomatique. Tallinn, la capitale a ensuite accueilli dès 2008 le centre de cyber défense de l'OTAN. Depuis, le pays a largement développé le vote électronique et la notion de e-gouvernement. Les projets de loi y sont mis en ligne dès leur présentation et la société civile est invitée à en débattre, initiative qui permet non seulement aux citoyens de s'engager pleinement dans la démocratie, mais de la comprendre. Comprendre son intérêt, ses enjeux, ses perspectives afin de mieux se l'approprier. Le système est même considéré comme un outil essentiel dans la lutte contre la corruption, c'est-à-dire la capacité d'une société à empêcher l'élite au pouvoir d'utiliser les ressources publiques et partagées. Une réforme née en 2012, a amené les enfants dès l'âge de sept ans à être formés au code informatique et sensibilisés aux outils numériques, pour leur apprendre très tôt à utiliser la technologie de manière intelligente.

Côté Europe de l'Ouest, on n'y est pas encore. Les quelques expériences de communication des pouvoirs publics donnent peu de résultats. En France, Tangui Morlier, cofondateur de l'association Regards citoyens et créateur du site www.nosdeputes.fr, estime que « *sur le site de l'Assemblée nationale, tout citoyen est invité à donner son opinion sur les études d'impact. Mais comme l'institution ne veut pas héberger des points de vue qui pourraient être litigieux, elle ne les met pas à disposition. Le citoyen peut contribuer, mais sa contribution n'est pas visible, et il ne sait pas ce qu'on en fait* ». Internet devient alors une illusion de démocratie participative. Peut-être l'IA pourrait-elle contribuer à la gestion de tous les avis et en faire remonter la substantielle moelle. Mais cela signifie aussi qu'on sous-traite ce travail à un système numérique opaque.

Et en Belgique, comment parler de démocratie numérique alors que, nous l'avons vu, bon nombre de personnes sont laissées au bord des routes d'Internet. Car on constate que la fracture numérique a augmenté la fracture sociale. L'illectronisme a aggravé l'illettrisme de personnes qui se sentaient déjà rejetées du débat démocratique. Et bientôt arrive l'IActronisme, car l'IA a un fonctionnement qui a des limites méconnues du grand public, comme sa capacité à inventer des informations comme nous l'avons vu plus haut. Il est donc important de pouvoir formuler des demandes à l'IA, les fameux prompts, en ayant connaissance de ces barrières et de son fonctionnement. Paradoxalement l'IA pourrait aider les personnes mal à l'aise avec l'écrit, et donc le numérique, à rédiger un courriel, voire à terme à remplir un formulaire avec une assistance IA. Cette dernière recevrait oralement les ordres et les demandes et les retranscrirait. Reste à savoir si ces aides resteront gratuites car, on le sait, « si c'est gratuit, c'est vous le produit ». Aujourd'hui déjà, les meilleures IA sont payantes. C'est sans doute sur ce genre de sujets que nos gouvernants ont un rôle à jouer : aider les plus isolés à se faire assister par l'IA pour leur permettre de se maintenir à flot administrativement et marginaliser les problèmes administratifs causés par l'analphabétisme.

Autre problème, cette nouvelle agora numérique est soumise à des surveillances, à des logiques algorithmiques, à des arnaques, à des harcèlements et, paradoxalement, à des polarisations

parfois violentes des débats… Car qui dit démocratie dit débat contradictoire, rencontre entre les citoyens qui n'ont pas tous la même opinion. Sur le Web, la différence fait fuir, l'internaute peut changer de page web comme il change de chemise. C'est lui qui choisit les idées sur lesquelles il veut débattre, et avec qui débattre. Et dans ce sens, comme dit Benjamin Barber, « le web nous dépolitise ! »[167]. Jean-Louis Missika, sociologue des médias, analyse le phénomène Internet. Il parle de « *multiplication des mondes propres* »[168]. Donner une opinion contradictoire dans un groupe amène régulièrement à une volée de bois vert. Les effets sur notre manière de débattre sont nombreux : la course à la visibilité algorithmique encourage une forme d'essentialisation des sujets, qui se voient résumés à une série de mots clés, souvent les plus rassembleurs pour améliorer leur audience. Cette perte de nuance conduit à une polarisation des discussions entre des camps fortement mobilisés.

D'ailleurs, la cyberdémocratie offre même la possibilité aux internautes de choisir les actualités qu'ils veulent suivre, ce qui revient à « consommer » une actualité « à la carte ». En 2023, un vaste sondage mené par l'Ifop, auprès des dix-huit/vingt-quatre ans français, pointait un constat qui doit nous faire réfléchir : « *plus la fréquence de consultation des réseaux sociaux (Twitter (X), TikTok…) est grande, plus l'adhésion aux contre-vérités augmente* »[169]. Les informations sont désormais soumises à l'acceptation du « client », elles doivent plaire, être faciles à comprendre (d'où le succès des complots) et digestes, à la manière d'une alimentation de fast-food mais, en l'occurrence, pour alimenter son esprit. Combien de fois n'entendons-nous pas en atelier ou en formation, que les médias donnent trop de mauvaises nouvelles ou qu'ils sont trop compliqués à comprendre ou encore qu'ils ne parlent pas de ce qu'il se passe réellement.

Internet est un danger pour la démocratie où le citoyen devient égocentrique

Certains les appellent les Merdias. Depuis quand les mass médias sont-ils le berceau des bonnes nouvelles, sont-ils des menteurs à la solde des pouvoirs ou parlent-ils de façon exhaustive d'absolument tout ce qui se passe en Belgique et dans le monde ? Depuis quand les problèmes géopolitiques, sociaux ou économiques doivent-ils être expliqués en cent cinquante caractères ? Cass Sunstein analyse l'Internet comme un danger pour la démocratie où le citoyen devient égocentrique, replié sur lui-même[170]. L'internaute a tendance à vivre dans son monde et sa croyance principale est qu'Internet est à la fois le progrès et la solution à tous les problèmes. Mais en s'isolant, le citoyen participe de moins en moins au débat public et le numérique lui fait plaisir en le confortant dans ses opinions, même les plus absurdes. À l'époque, une personne qui prétendait que la terre était plate ou que Poutine était un pacifiste, était vite recadré par son entourage. Aujourd'hui, nous pouvons tous trouver des milliers de personnes qui partagent notre avis à travers le monde, et être conforté dans l'idée que notre entourage est dans l'ignorance. Si Internet est le meilleur outil de recherche au monde, il est aussi le chantre de l'irrationnel.

Et comment imaginer un débat public serein quand des citoyens font face à l'omniprésence des arnaques, des théories complotistes, des infox, des discours extrémistes banalisés ou des propagandes de tout type ?

Le débat public dépend donc beaucoup trop du médium, des intervenants, de ceux qui en ont le contrôle, de leur fonctionnement et d'une illusion de démocratie dans de nombreux cas… Pour pouvoir s'exprimer dans cette jungle numérique, il faut un nombre de connaissances croissant pour suivre les évolutions technologiques ultra-rapides et surtout se prémunir des biais et des abus en tout genre. Or, à ce jour, nous sommes encore frappés par le nombre de personnes qui ne savent pas ce qu'est un cookie informatique et en quoi les refuser les protège[171], ou encore par ceux qui ne savent pas ce que sont les algorithmes, qui guident pourtant leurs choix au quotidien. Rappelons également que si 10 % des Belges ont encore des difficultés à lire et à écrire, d'autres rencontrent des difficultés avec l'usage fréquent de l'anglais dans les énoncés et les expressions en usages sur le net. D'ailleurs combien de personnes aujourd'hui ont entendu parler de *quishing*[172], d'abus de type « use-after-free »[173], d'un data broker[174] ou s'intéressent à ses privacy settings[175] et pensent à faire des back-up[176] ?

Gageons que les nouvelles législations européennes puissent permettre de limiter les effets néfastes de ces réseaux pour que nous puissions jouir ainsi uniquement de leurs qualités indéniables. Nous éviterions ainsi une démocratie essentiellement algorithmique au profit de celle exercée par des peuples libres et conscientisés.

Conclusions

Nous le voyons, il y a encore de très nombreux défis à relever pour que la transition numérique respecte les règles démocratiques.

« *La démocratie doit-elle s'adapter au numérique ou le numérique doit-il s'adapter à la démocratie ? La réponse semble évidente, pourtant, dans les faits, les choses sont plus floues* » soulignait Elise Degrave. Si certains ont comparés l'arrivée d'Internet à celle de l'imprimerie ou de la radio, et de leur influence sur la manipulation des masses, aucun de ces médias ne s'est autant immiscé dans la vie privée des citoyens, aucun n'a permis un espionnage de tout

utilisateur et bafoué à ce point les lois des États démocratiques. D'autant que les personnalités politiques ont fait preuve de naïveté à son égard.

Aujourd'hui, les démocraties doivent lutter contre des plateformes monopolistiques et leur liberté d'expression… du business, contre des arnaques et des propagandes en expansion, contre des sélections algorithmiques opaques, contre des tentations de cyber et data surveillances, contre les bulles de filtres, contre une course à la visibilité algorithmique qui encourage une forme d'essentialisation des sujets résumés à une série de mots clés, souvent les plus rassembleurs pour améliorer l'audience, contre une perte de la nuance et du débat constructif, contre des extrémismes décomplexés, contre la fracture numérique sociale, contre une course au « techno-solutionnisme » effrénée, contre une ubérisation de l'économie qui contourne nos lois sociales et le financement de nos institutions… Et nous n'avons même pas parlé ici d'autres problèmes qui sont analysés dans différents articles de ce cahier numérique, comme les limites matérielles, environnementales et sociales de la course au numérique, la dépendance à tous ces outils, les problèmes de santé mentale et physique ou encore de biais de programmation.

Et désormais, l'IA amène de nouvelles solutions mais aussi de nouveaux problèmes, que ce soit pour la compréhension de l'outil et son utilisation ou pour le perfectionnement des arnaques et de la désinformation. Cette course, pour ne pas être distancés par d'autres États plus avancés technologiquement, entraîne des dégâts visibles et collatéraux qui devront être comblés, la plupart du temps par des investissements publics, que ce soit pour des pertes financières de l'ubérisation de notre économie, pour éduquer aux nouvelles technologies, pour lutter contre le harcèlement, pour lancer des poursuites judiciaires contre des crimes en ligne, pour tenir à jour ses équipements et leur sécurité, pour investir dans des technologies évoluant sans cesse ou pour lutter contre des problèmes de santé physiques (myopie[177], obésité…) ou mentales (dépendances, harcèlement, adhésion aux contre-vérités…).

Le numérique offre des outils puissants pour améliorer la démocratie en facilitant l'expression des libertés individuelles et collectives mais ils sont mal utilisés, voire dévoyés. Nombre de décideurs politiques sont aujourd'hui dépassés et s'en réfèrent à des techniciens et des programmateurs, voire à des logiciels opaques, peu en contact avec les réalités de nombreux citoyens. Oui, il faut certes éduquer aux médias mais peut-être devrait-on commencer par nos dirigeants, qui se montrent un peu trop légers avec la question de nos données personnelles, et sont même prêts à bafouer des lois en période de crise, comme souligné plus haut par Philippe Laloux et Elise Degrave, lors de la crise de la Covid-19. Il est vrai que les GAFAM arrivent à récolter plus d'informations sur les Belges que l'État lui-même. Ce dernier doit en effet respecter les garde-fous démocratiques mis en place par les élus. Tout comme les journalistes doivent respecter une déontologie et vérifier leurs sources.

Un paradoxe, qui montre la puissance des plateformes. D'autant que leurs algorithmes informent et remplacent de plus en plus la presse, autre garant démocratique, chez de nombreux citoyens. L'info doit-elle devenir un produit de consommation ayant autant de valeur qu'un récit conspiratrionniste capillotracté ? Et les programmes et les débats politiques doivent-ils devenir des arènes d'acrimonies et de *punch lines* polarisées pour divertir le peuple ? Doit-on tout privatiser, jusqu'à la pensée de nos jeunes, jusqu'à notre vie sociale et jusqu'au sacrifice de nos outils démocratiques ? Le business de la peur et de l'émotion, ainsi que l'économie de l'attention sont-ils l'avenir de nos systèmes de pensées ? Et notre vie privée a-t-elle encore un avenir ? Ce sera un combat de tous les jours pour les États, mais certains pourront se protéger mieux que d'autres.

Bien des choses doivent évoluer. Or, l'UE est sans doute le meilleur défenseur au monde de nos droits face aux mastodontes que sont les GAFAM, NATU et autres BATX, qui détiennent un pouvoir considérable face à l'information et la participation citoyenne. L'influence de ces derniers peut même rivaliser avec celle des États, remettant en cause la souveraineté des gouvernements et leur capacité à protéger les intérêts publics. Une UE qui doit faire front et résister. Si toutefois son pouvoir ne se retrouve pas entre les mains des extrêmes droites, qui pourraient avoir une vision « Muskienne » des réseaux sociaux.

Et, pendant que nous finissions cette étude, Elon Musk est devenu membre du gouvernement Trump, partageant son libertarianisme très personnel, puisque liberticide sur des sujets comme la migration, l'homosexualité, la place des femmes, le journalisme qualitatif, l'avortement ou la transsexualité. Nul doute que l'Europe se dirige vers un bras de fer encore plus complexe avec ce nouveau gouvernement US pour faire respecter nos RGPD, DMA, DSA et autres IA-Act. D'autant que Brendan Carr a été nommé à la tête de la FCC, le régulateur américain des télécoms. Son objectif, supprimer la censure et forcer les GAFAM à suivre la totale liberté d'expression façon X, soit celle d'Elon Musk. Cela va à l'exacte opposé de la direction prise par l'UE sur la désinformation et les appels à la haine. Donald Trump pourrait menacer l'UE de sanctions économiques, comme de fortes taxes sur les importations, pour la faire plier. Désormais, nous utilisons des réseaux sociaux et des outils numériques souvent programmés dans des pays qui n'ont pas la même vision de la démocratie que nous, comme la Chine,

les États-Unis ou la Russie. L'UE va devoir être forte et créative pour faire respecter ses idées et ses règles démocratiques, ainsi que pour protéger ses citoyens et ses marchés.

Le défi est énorme et nous nous inquiétons particulièrement des États non démocratiques et/ou en développement, qui n'ont pas d'éducation aux médias et subissent des pressions politiques, de la propagande, de la cybersurveillance.

Comme souligné en introduction de cette étude, une boîte de Pandore a été ouverte, libérant de nombreux problèmes, directement ou indirectement liés aux principes démocratiques. Un simple exemple : qui se soucie aujourd'hui des modérateurs de contenus ? Ces employés des réseaux sociaux qui passent leur journée à faire le tri entre des images acceptables et des images violentes, jusqu'à l'insoutenable (tortures, suicides, actes pédophiles, viols, assassinats, suprémacisme, harcèlements…). En octobre 2023, un article EuroNews annonçait qu'en Espagne, « *Des employés de Meta poursuivent l'entreprise en justice. Plus de 20 % du personnel engagé par Meta pour vérifier le contenu violent de Facebook et d'Instagram est en arrêt maladie pour cause de traumatisme psychologique* »[178]. Pourquoi ces métiers sont-ils tolérés en démocratie ? Qui va financer leurs thérapies ?

Et que dire du dark net, cet Internet opaque, mal connu des citoyens, utilisé par des réseaux criminels et accessible à toute personne un peu débrouillarde avec l'outil ? À l'inverse, nous sommes tous des proies potentielles pour les arnaques, le chantage et le piratage.

Nos démocraties ont donc encore beaucoup de travail pour contrer les attaques, les malveillances et les dommages du net, et trouver une forme de « souveraineté numérique ». Cela passera par des investissements dans une éducation au numérique efficace, dans des outils plus transparents et sécurisés, dans une gestion éthique des datas, dans des garde-fous législatifs solides et désormais dans une IA fiable. Mais il nous semble qu'il reste un long chemin à parcourir. En attendant, nous conclurons par une phrase d'une fervente défenseuse de notre démocratie belge, Elise Degrave : « *A l'instar de l'AFSCA qui contrôle la chaîne alimentaire, il faudrait créer une autorité indépendante de contrôle des algorithmes. Des décisions importantes qui concernent tout le monde sont pour le moment hors de contrôle. On ne peut pas accepter dans un État de droit d'être gouverné par des algorithmes secrets et non contrôlés. Il faudra sans doute des années pour faire bouger les lignes. Mais nous sommes de plus en plus de chercheurs à le défendre et cela en vaut la peine pour que le numérique soit mis à la bonne place, celle d'un outil au service de la société* »[179].

[1] BATX est un sigle formé sur le modèle de GAFAM (Google, Amazon, Facebook, Apple, Microsoft) en juxtaposant les initiales des quatre entreprises du Web chinois : Baidu, Alibaba, Tencent et Xiaomi.

[2] Apparu durant l'été 2015, ce nouvel acronyme désigne les quatre fantastiques de la nouvelle vague technonumérique que sont Netflix, Airbnb, Tesla et Uber.

[3] ETX, « Des lentilles connectées pour profiter de la réalité augmentée », Les Numériques, le 10 juillet 2022, [en ligne :] https://www.lesnumeriques.com/casque-realite-virtuelle/des-lentilles-connectees-pour-profiter-de-la-realite-augmentee-n187331.html, consulté le 12 juillet 2024.

[4] Rosanvallon P., « Réinventer la démocratie », SES.ENS-Lyon, 09 février 2009, [en ligne :] https://ses.ens-lyon.fr/articles/pierre-rosanvallon-reinventer-la-democratie--62763, consulté le 30 août 2024.

[5] Courteille P., « Fakeland, un nouvel et obscur continent », Citoyenneté & Participation, Étude n°31, avril 2020, [en ligne :] https://www.cpcp.be/publications/fakeland.

[6] Diffusé dans l'émission Doc Shot sur la Une, RTBF, le 13 juin 2024 à 22h35.

[7] Kanter J., « Former Guardian editor: Facebook sucked up £20 million of our online ad revenue last year », Business Insider, le 5 septembre 2016, [en ligne :] https://www.businessinsider.com/alan-rusbridger-blames-facebook-guardian-digital-revenue-2016-9?op=1, consulté le 20 juillet 2024.

[8] L'extrême droite américaine.

[9] Rodriguez S., « Meta Has Run Hundreds of Ads for Cocaine, Opioids and Other Drugs », Wall Street Journal, 31 juillet 2024, [en ligne :] https://www.wsj.com/tech/meta-cocaine-opioids-ads-dea8e0fc, consulté le 10 août 2024

[10] Bibliothèque de publicités Meta, [en ligne :] https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=ALL&media_type=all&q=high%20supplies&search_type=keyword_unordered.

[11] Olcina J., « Facebook, Instagram, X : pourquoi les réseaux sociaux sont remplis d'arnaques », Geecko (LeSoir), 7 août 2024, [en ligne :] https://geeko.lesoir.be/2024/08/07/facebook-instagram-x-pourquoi-les-reseaux-sociaux-sont-remplis-darnaques, consulté le 21 août 2024.

[12] Untersinger M., Reynaud F. et Piquard A., « "Facebook Files" : Frances Haugen, lanceuse d'alerte nouvelle génération », Le Monde, 8 novembre 2021, [en ligne :] https://www.lemonde.fr/pixels/article/2021/11/08/facebook-files-frances-haugen-lanceuse-d-alerte-nouvelle-generation_6101330_4408996.html, consulté le 26 juillet 2024.

[13] Reynaud F., « Comment un même écosystème nourrit campagnes de désinformation et cybercriminalité », Le Monde, le 11 juillet 2024, [en ligne :] https://www.lemonde.fr/pixels/article/2024/07/11/comment-un-meme-ecosysteme-nourrit-campagnes-de-desinformation-et-cybercriminalite_6248473_4408996.html, consulté le 19 août 2024.

[14] *Ibid.*

[15] La rédaction de Francetvinfo, « On vous explique l'affaire des réseaux pédophiles qui agite YouTube », France Tv Info, 25 février 2019, [en ligne :] https://www.francetvinfo.fr/internet/reseaux-sociaux/on-vous-explique-l-affaire-des-reseaux-pedophiles-qui-agite-YouTube_3206817.html, consulté le 20 août 2024.

[16] Tiré du documentaire « Le piège du clic » de Peter Porta, diffusé dans l'émission Doc Shot sur la Une, RTBF, le 13 juin 2024 à 22h35.

[17] Page d'accueil d'Algotransparancy, [en ligne :] https://www.algotransparency.org, consulté le 24 août 2024.

[18] Reisacher A., « Chiffres YouTube : les statistiques à connaître en 2024 », Le blog du modérateur, le 12 février 2024, [en ligne :] https://www.blogdumoderateur.com/chiffres-YouTube/, consulté le 25 août 2024.

[19] Berr J., « why many internet ads are never seen by anyone », CBS News, le 3 décembre 2014, [en ligne :] https://www.cbsnews.com/news/why-many-internet-ads-are-never-seen-by-anyone, consulté le 27 août2024.

[20] Une ferme à clics est une personne ou une organisation faisant commerce des « likes », des « vues » ou et des « followers ». En général des personnes précarisées d'Asie qui alimentent en clics des sites de clients en Occident, leurs donnant ainsi artificiellement une impression de succès public.

[21] Benoit F., « Le business de la pub en ligne est bâti sur une fiction : son efficacité », Usbek et Rita, le 15 mars 2022, [en ligne :] https://usbeketrica.com/fr/article/le-business-de-la-pub-en-ligne-est-bati-sur-une-fiction-son-efficacite, consulté le 27 août 2024.

[22] *Ibid.*

[23] Torres J., « Pubs ciblées : pour les usagers et la concurrence, la fin de la collecte des données sur Meta représenterait "un tournant majeur" », Libération, le 3 novembre 2023, [en ligne :] https://www.liberation.fr/economie/economie-numerique/pubs-ciblees-pour-les-usagers-et-la-concurrence-la-fin-de-la-collecte-des-donnees-sur-meta-representerait-un-tournant-majeur-20231103_DFXDFXD5SBFN5E67VRAM6JARUE, consulté le 22 juillet 2024.

[24] Reynaud F., « TikTok condamné à une amende de 345 millions d'euros en Europe pour ne pas avoir protégé les données de ses utilisateurs », Le Monde, le 15 septembre 2023, [en ligne :] https://www.lemonde.fr/pixels/article/2023/09/15/protection-des-donnees-tiktok-condamne-a-une-amende-de-345-millions-d-euros_6189547_4408996.html, consulté le 22 juillet 2024.

[25] Voir l'étude d'Emma Raucent, « Le travail sous l'ère du capitalisme de plateforme », août 2022, [en ligne :] https://www.cpcp.be/publications/capitalisme-plateforme, consulté en septembre 2022.

[26] Encinas L., « NATU : les 4 fantastiques de la nouvelle vague technonumérique », Usbek et Rita, le 2 mai 2017, [en ligne :] https://usbeketrica.com/fr/article/natu-les-4-fantastiques-de-la-nouvelle-vague-technonumerique, consulté le 19 juillet 2024.

[27] Cloot A., « Comment Booking.com ne paie quasi pas d'impôts en Belgique », Le Soir, le 31 juillet 2017, [en ligne :] https://www.lesoir.be/107084/article/2017-07-31/comment-bookingcom-ne-paie-quasi-pas-dimpots-en-belgique, consulté le 18 juillet 2024.

[28] Henni J., « L'impôt minuscule (encore) payé par Google en France l'an passé », Capital, le 18 août 2021, [en ligne :] https://www.capital.fr/entreprises-marches/limpot-minuscule-paye-par-google-en-france-lan-passe-1412194, consulté le 25 juillet 2024.

[29] Agence Belga, « Commerce : Google reconnu coupable de pratiques anticoncurrentielles, estime un juge américain », RTBF, 6 août 2024, [en ligne :] https://www.rtbf.be/article/commerce-google-reconnu-coupable-de-pratiques-anticoncurrentielles-estime-un-juge-americain-11416343, consulté le 8 août 2024.

[30] *Ibid.*

[31] « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) », Journal officiel de l'Union européenne, le 27 avril 2016, [en ligne :] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679, consulté le 9 août 2024.

[32] La rédaction, « DMA : le règlement sur les marchés numériques veut mettre fin à la domination des géants du Net », Vie Publique, le 13 mai 2024, [en ligne :] https://www.vie-publique.fr/eclairage/284907-dma-le-reglement-sur-les-marches-numeriques-ou-digital-markets-act, consulté le 23 juillet 2024.

[33] Cette analyse fait partie de ce cahier, Fronteddu B., « Donner ses données ? », Citoyenneté & Participation, analyse n°473, juillet 2023, [en ligne :] https://www.cpcp.be/publications/donner-donnees-personnelles, consulté en septembre 2023.

[34] Leith D. J., « Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple and Google », School of Computer Science & Statistics, Trinity College Dublin-Ireland, le 25 mars 2021, [en ligne :] https://www.scss.tcd.ie/doug.leith/pubs/apple_google2.pdf, consulté le 25 juillet 2024.

[35] La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée et informatique, ni aux libertés individuelles ou publiques.

[36] L'Institut national de recherche en informatique et en automatique (Inria), ou « institut national de recherche en sciences et technologies du numérique », est un établissement public français à caractère scientifique et technologique spécialisé en mathématiques et informatique.

[37] Étude de la CNIL et de l'Inria, « Mobilitics, découvrir la partie immergée de l'iceberg des apps pour smartphone », CNIL, Novembre 2014, [en ligne :] https://linc.cnil.fr/mobilitics-decouvrir-la-partie-immergee-de-liceberg-des-apps-pour-smartphone, consulté le 25 juillet 2024.

[38] Clairouin O. et Untersinger M., « Meta condamné à une amende record de 1,2 milliard d'euros par le régulateur irlandais des données personnelles », Le Monde, le 22 mai 2023, [en ligne :] https://www.lemonde.fr/pixels/article/2023/05/22/meta-condamne-a-une-amende-record-de-1-2-milliard-d-euros-par-le-regulateur-irlandais-des-donnees-personnelles_6174333_4408996.html, consulté le 25 juillet 2024.

[39] Six N., « Données personnelles : des associations européennes de consommateurs portent plainte contre Google », Le Monde, le 1er juillet 2022, [en ligne :] https://www.lemonde.fr/pixels/article/2022/07/01/donnees-personnelles-des-associations-europeennes-de-consommateurs-portent-plainte-contre-google_6132915_4408996.html, consulté le 25 juillet 2024.

[40] Créée en 1973, SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une société privée de droit belge qui offre une plate-forme de messagerie sécurisée, des standards pour communiquer et un bouquet de produits et de services autour de cette messagerie. Ce réseau est principalement utilisé pour transmettre des informations pour réaliser des virements bancaires.

[41] Dèbes F., « Données personnelles : la somme des amendes contre Meta s'approche du milliard d'euros », Les Echos, le 28 novembre 2022, [en ligne :] https://www.lesechos.fr/tech-medias/hightech/donnees-personnelles-la-somme-des-amendes-contre-meta-sapproche-du-milliard-deuros-1883576, consulté le 26 juillet 2024.

[42] La rédaction de la RTBF, « Les accès de 3,2 millions d'utilisateurs belges de WhatsApp piratés et revendus sur le dark web. Comment se protéger ? », RTBF, le 21 août 2024, [en ligne :] https://www.rtbf.be/article/les-acces-de-3-2-millions-d-utilisateurs-belges-de-whatsapp-pirates-et-revendus-sur-le-darkweb-comment-se-proteger-11422978, consulté le 2 septembre 2024.

[43] La rédaction du Soir, « 92% des membres de Linkedin victimes d'une fuite de données : les conseils de la Computer Crime Unit », Le Soir, le 24 octobre 2021, [en ligne :] https://www.lesoir.be/402408/article/2021-10-24/92-des-membres-de-linkedin-victimes-dune-fuite-de-donnees-les-conseils-de-la, consulté le 26 juillet 2024.

[44] Ainsi 1,4 milliard de données viendraient de Tencent QQ (une application chinoise de messagerie instantanée) et 504 millions de Weibo. Cela n'empêche pas des sites plus connus chez nous d'être aussi concernés. On citera par exemple Twitter (281 millions), Deezer (258 millions), LinkedIn (251 millions), Adobe (153 millions), Canva (143 millions), Daily Motion (86 millions) ou encore Dropbox (69 millions).

[45] Lefevre M., « La pire fuite de données de l'histoire : voici comment vérifier si vous êtes concerné(e) », Trends Tendance, le 24 janvier 2024, [en ligne :] https://trends.levif.be/a-la-une/tech-medias/la-pire-fuite-de-donnees-de-lhistoire-voici-comment-verifier-si-vous-etes-concernes, consulté le 2 août 2024.

[46] Fleureau G., « X lance Trend Genius, un nouvel outil de publicité contextuelle », Siècle Digital, 23 juillet 2024, [en ligne :] https://siecledigital.fr/2024/07/23/x-lance-trend-genius-un-nouvel-outil-de-publicite-contextuelle, consulté le 8 août 2024.

[47] Bezat J-M., « Dans le cloud, il faut désormais coopérer avec les Gafam tout en protégeant les données », Le Monde, le 16 novembre 2021, [en ligne :] https://www.lemonde.fr/economie/article/2021/11/16/dans-le-cloud-il-faut-desormais-cooperer-avec-les-gafam-tout-en-protegeant-les-donnees_6102261_3234.html, consulté le 9 août 2024.

[48] Hill K, « The Secretive Company That Might End Privacy as We Know It », 18 janvier 2020, [en ligne :] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, consulté le 5 août 2024.

[49] Van Roelen M., « 51 organisations demandent l'interdiction de la reconnaissance faciale en Europe », Geeko (Le Soir), le 7 avril 2021, [en ligne :] https://geeko.lesoir.be/2021/04/07/51-organisations-demandent-linterdiction-de-la-reconnaissance-faciale-en-europe, consulté le 12 août 2024.

[50] *Ibid.*

[51] Ce projet du gouvernement chinois vise à mettre en place un système national de réputation des citoyens et des entreprises, en y ajoutant un système de récompenses et de pénalités pour ceux respectant ou ne respectant pas les règles édictées. Le système repose sur des outils de surveillance globale et de surveillance de masse, et utilise les technologies d'analyse du big data, afin d'établir un réseau de « confiance » (守信, shǒuxìn). Mais le système est également un instrument politique, destiné à étouffer les critiques du régime.

[52] Courteille P., « Fakeland, un nouvel et obscur continent », Citoyenneté & Participation, *op. cit.*

[53] La rédaction d'Amnesty International, « Les "Facebook Papers": quelles conséquences sur les droits humains ? », Amnesty International, le 4 novembre 2021, [en ligne :] https://www.amnesty.org/fr/latest/campaigns/2021/11/the-facebook-papers-what-do-they-mean-from-a-human-rights-perspective, consulté le 12 août 2024.

[54] Six N., « Massacre des Rohingya : "Facebook a joué un rôle central dans la montée du climat de haine" en Birmanie », Le Monde, le 29 septembre 2022, [en ligne :] https://www.lemonde.fr/pixels/article/2022/09/29/massacre-des-rohingya-facebook-a-joue-un-role-central-dans-la-montee-du-climat-de-haine-en-birmanie_6143611_4408996.html, consulté le 23 juillet 2024.

[55] Selon Patrick Brùn, l'avocat et chercheur Patrick de Brún, auteur du rapport d'Amnesty, Facebook « a reçu des dizaines d'avertissements. Des acteurs locaux ont rapidement signalé les campagnes de messages haineux orchestrées par les militaires et leurs alliés, comme le Ma Ba Tha, l'association pour la protection de la race et de la religion. D'année en année, des militants des droits humains et des chercheurs d'universités occidentales ont lancé de nouvelles alertes, allant jusqu'à se déplacer au siège de Facebook. Le message porté était le suivant : si rien n'est fait, la Birmanie pourrait devenir le nouveau Rwanda. Selon plusieurs employés de Facebook que nous avons interrogés, il est impossible que ces messages n'aient pas été entendus dans les hautes sphères de l'entreprise.

[56] La rédaction d'Amnesty International, « L'atrocité des réseaux sociaux », Amnesty International, le 29 septembre 2022, [en ligne :] https://www.amnesty.org/fr/documents/asa16/5933/2022/fr, consulté le 24 juillet 2024.

[57] Rodo F., « Des réfugiés rohingyas portent plainte contre Facebook », France 24, le 7 décembre 2021, [en ligne :] https://www.france24.com/fr/asie-pacifique/20211207-des-r%C3%A9fugi%C3%A9s-rohingyas-portent-plainte-contre-facebook, consulté le 24 juillet 2024.

[58] Voir Amnesty International, « Kenya. Meta est poursuivie à hauteur de 1,5 milliard d'euros pour avoir alimenté la violence ethnique en Éthiopie », le 14 décembre 2022, [en ligne :] https://www.amnesty.org/fr/latest/news/2022/12/kenya-meta-sued-for-1-6-billion-usd-for-fueling-ethiopia-ethnic-violence, consulté le 26 août 2024.

[59] The Verge est un site américain lancé le 21 octobre 20111 qui traite de l'actualité technologique, de l'information et des médias.

[60] La rédaction d'Amnesty International, « Les "Facebook Papers" : quelles conséquences sur les droits humains? », *op. cit.*

[61] Le TTP est un centre d'information et de recherche pour les journalistes, les universitaires, les décideurs et les membres du public s'intéressant à l'influence des principales plateformes technologiques sur la politique et la société.

[62] Voir documentaire Le piège du clic, de Peter Porta, diffusé dans l'émission Doc Shot sur la Une, RTBF, le 13 juin 2024 à 22h35.

[63] Agence Belga, « Un syndicat annonce porter plainte contre Trump et Musk pour "tentative d'intimidation" », La Libre Belgique, le 13 août 2024, [en ligne :] https://www.lalibre.be/international/amerique/2024/08/13/un-syndicat-annonce-porter-plainte-contre-trump-et-musk-pour-tentative-dintimidation-YHGE574T2RGILDC67OV6AWO7NA, consulté le 22 août 2024.

[64] Zhuang Y. et Ward E., « Twitter Reinstates Suspended Accounts of Several Journalists », New York Times, le 17 décembre 2022, [en ligne :] https://www.nytimes.com/2022/12/17/business/media/twitter-reinstates-accounts.html, consulté le 13 août 2024.

[65] Oracle (Oracle Corporation) : son produit phare est le système de gestion de base de données Oracle Database. En 2019, Oracle était la deuxième plus grande entreprise de logiciels en matière de chiffre d'affaires et de capitalisation boursière, selon Forbes. [en ligne :] https://www.forbes.com/consent/ketch/?toURL=https://www.forbes.com/global2000/list/#industry:Software%20%26%20Programming, consulté le 23 août 2024.

[66] Del'Arizona, du Michigan, de la Géorgie, de la Caroline du Nord, du Nevada, de la Pennsylvanie et du Wisconsin.

[67] Schwartz B., « How an Elon Musk PAC is using voter data to help Trump beat Harris in 2024 election », CNBC, le 2 août 2024, [en ligne :] https://www.cnbc.com/2024/08/02/elon-musk-pac-voter-data-trump-harris.html, consulté le 18 août 2024.

[68] Mattioli D., Palazzolo J., Glazer E., « Inside Elon Musk's Hands-On Push to Win 800,000 Voters for Trump », The Wall Street Journal, le 12 août 2024, [en ligne :] https://www.wsj.com/politics/elections/inside-elon-musks-hands-on-push-to-win-800-000-voters-for-trump-0a7d55b3, consulté le 22 août 2024.

[69] Reuters, « Musk-backed PAC under investigation for potential violations of Michigan laws », Reuters, le 5 août 2024, [en ligne :] https://www.reuters.com/world/us/musk-backed-pac-under-investigation-potential-violations-michigan-laws-2024-08-04, consulté le 22 août 2024.

[70] Schwartz B., « How an Elon Musk PAC is using voter data to help Trump beat Harris in 2024 election », *op. cit.*

[71] La Première, « Elon Musk, un imposteur de la tech et agresseur ? Les mensonges et travers du multimilliardaire », RTBF, le 30 mai 2024, [en ligne :] https://www.rtbf.be/article/elon-musk-un-imposteur-de-la-tech-et-agresseur-les-mensonges-et-travers-du-multimilliardaire-11380925, consulté le 22 août 2024.

[72] RFI, « Elon Musk fait un don considérable pour la campagne de Donald Trump », RFI, 13 juillet 2024, [en ligne :] https://www.rfi.fr/fr/am%C3%A9riques/20240713-elon-musk-fait-un-don-consid%C3%A9rable-campagne-trump-presidentielle-usa, consulté le 22 août 2024.

[73] AFP, « "Guerre civile", "Union soviétique": en pleines émeutes, Musk défie le gouvernement britannique », La Libre Belgique, le 6 août 2024, [en ligne :] https://www.lalibre.be/international/europe/2024/08/06/guerre-civile-union-sovietique-en-pleines-emeutes-musk-defie-le-gouvernement-britannique-N5SGDRKVBNHMHF53XHPNQY7RLA, consulté le 24 août 2024.

[74] Dougnac V., « Présidentielle américaine 2024 : Elon Musk, influenceur hors-norme en informations politiques trompeuses », La Croix, le 9 août 2024, [en ligne :] https://www.la-croix.com/international/presidentielle-americaine-2024-elon-musk-influenceur-hors-norme-en-informations-politiques-trompeuses-20240809, consulté le 22 août 2024.

[75] Thiombane D., « L'histoire des bébés avortés et mangés dans la soupe à Pékin est fausse », AfricaCheck, le 31 janvier 2020, [en ligne :] https://africacheck.org/fr/fact-checks/meta-programme-fact-checks/lhistoire-des-bebes-avortes-et-manges-dans-la-soupe-pekin, consulté le 30 août 2024.

[76] Fried A., « Elon Musk offre chaque jour un million à un signataire d'une pétition pro-Trump : est-ce légal ? », Europe 1, le 23 octobre 2024, [en ligne :] https://www.europe1.fr/international/elon-musk-offre-chaque-jour-un-million-a-un-signataire-dune-petition-pro-trump-est-ce-legal-4274484, consulté le 1 novembre 2024.

[77] Kinder T., Hammond G. et Murphy H., in San Francisco, et Rogers A. in Milwaukee, « Has Silicon Valley gone Maga? », Financial Times, 19 juillet 2024, [en ligne :] https://www.ft.com/content/e2ffd807-1c18-436c-9f70-2fa7181ace2a, consulté le 6 août 2024.

[78] Comme le souligne Olivier Alexandre, chercheur du CNRS au Centre Internet et Société (CIS) et auteur de La Tech. Quand la Silicon Valley refait le monde (Seuil, 2023) : « L'administration Biden a instauré des mesures de régulation de l'intelligence artificielle avec un cadre assez ferme. Elle a resserré les mailles de la loi antitrust de Sherman [qui vise à limiter ou réduire la concentration économique] en lançant des enquêtes sur plusieurs poids lourds de la tech via la Federal Trade Commission (FTC). En 2022, quand le président américain a annoncé la mise en place de normes RSE [responsabilité sociétale des entreprises] dans l'encadrement des fonds de pension, il a déclenché une levée de boucliers chez les investisseurs. Ces derniers mois, il a prévu une taxe à hauteur de 25 % sur les plus-values latentes. Selon les capital-risqueurs de la Silicon Valley, qui lèvent de l'argent auprès de grandes fortunes, de grands comptes, de fonds de pension, ces mesures représentent un risque quasi existentiel. Il n'est pas question de la politique sociale ou internationale de Donald Trump, mais d'une administration Biden perçue comme hostile à leur industrie ».

[79] RTL Info et AFP, « Des contenus censurés sur les réseaux pendant la pandémie du Covid ? Mark Zuckerberg révèle une "erreur" », RTL Info, 27 août 2024, [en ligne :] https://www.rtl.be/actu/monde/international/des-contenus-censures-sur-les-reseaux-pendant-la-pandemie-du-covid-mark/2024-08-27/article/704344, consulté le 3 septembre 2024.

[80] Reuters, « Musk-backed PAC under investigation for potential violations of Michigan laws », *op. cit.*

[81] Wendling M., « How Musk and Trump put aside their differences », BBC, 12 août 2024, [en ligne :] https://www.bbc.com/news/articles/cvgd08np9z1o, consulté le 22 août 2024.

[82] Wendling M., « Ce que l'on sait de JD Vance, le choix de Trump pour la vice-présidence », BBC, le 13 octobre 2024, [en ligne :] https://www.bbc.com/afrique/articles/c8697y2dggpo, consulté le 24 octobre 2024.

[83] QAnon est une mouvance conspirationniste d'extrême droite venue des États-Unis, regroupant les promoteurs de théories du complot selon lesquelles une guerre secrète a lieu entre Donald Trump et des élites implantées dans le gouvernement (l'État profond ou Deep State), les milieux financiers et les médias, qui commettraient des crimes pédophiles, cannibales et sataniques

[84] AFP et 20 Minutes, « Elon Musk va déplacer les sièges sociaux de SpaceX et X en réaction à une loi sur les élèves transgenres », 20 Minutes, 17 juillet 2024, [en ligne :] https://www.20minutes.fr/monde/4101727-20240717-elon-musk-va-deplacer-sieges-spacex-x-apres-loi-eleves-transgenres, consulté le 23 août 2024.

[85] Le Monde avec AP, AFP et Bloomberg, « Elon Musk va déplacer les sièges de X et de SpaceX au Texas pour protester contre une loi protégeant les personnes transgenres en Californie », Le Monde, 16 juillet 2024, [en ligne :] https://www.lemonde.fr/international/article/2024/07/16/elon-musk-va-deplacer-les-sieges-de-x-et-de-spacex-au-texas-en-reaction-a-une-loi-sur-les-personnes-transgenres-en-californie_6251221_3210.html, consulté le 23 août 2024.

[86] AFP et 20 Minutes, « Elon Musk va déplacer les sièges sociaux de SpaceX et X en réaction à une loi sur les élèves transgenres », *op. cit.*

[87] Coëffé T., « Chiffres Twitter – 2024 », Blog du modérateur, 4 mars 2024, [en ligne :] https://www.blogdumoderateur.com/chiffres-twitter, consulté le 23 août 2024.

[88] La rédaction d'Euronews, « Une nouvelle salve de 22 satellites Starlink lancés en orbite basse », Euronews, le 8 janvier 2024, [en ligne :] https://fr.euronews.com/2024/06/08/une-nouvelle-salve-de-22-satellites-starlink-lances-en-orbite-basse, consulté le 23 août 2024.

[89] Trinel S., « La Chine lance sa constellation de satellites rivale de Starlink », BFM Tech & co, 6 août 2024, [en ligne :] https://www.bfmtv.com/tech/vie-numerique/la-chine-lance-sa-constellation-de-satellites-rivale-de-starlink_AV-202408060335.html, consulté le 23 août 2024.

[90] Kleinman Z., « Twitter wrong to block tweets during Turkey election – Wikipedia founder », BBC, le 16 mai 2023, [en ligne :] https://www.bbc.com/news/technology-65609123, consulté le 24 août 2024.

[91] Pearson J., « 'Free Speech Absolutist' Elon Musk Censors BBC Doc Critical of India's PM on Twitter », Vice, le 25 janvier 2023, [en ligne :] https://www.vice.com/en/article/free-speech-elon-musk-censors-bbc-doc-india-modi, consulté le 24 août 2024.

[92] La rédaction de la RTBF avec Agence, « Présidentielle américaine 2024 : l'UE met en garde Musk avant son interview sur X en direct avec Trump », RTBF Info, le 12 août 2024, [en ligne :] https://www.rtbf.be/article/presidentielle-americaine-2024-l-ue-met-en-garde-musk-avant-son-interview-sur-x-en-direct-avec-trump-11420048, consulté le 24 août 2024.

[93] Selon Forbes, au 1er juin 2024, la fortune d'Elon Musk est estimée à un peu plus de 210 milliards de dollars.

[94] Une distinction créée en 1988 par le Parlement européen pour honorer les personnes ou les organisations qui ont consacré leur existence à la défense des droits de l'homme et des libertés fondamentales

[95] Mendret M., « Le combat entre un juge brésilien et Elon Musk à propos de la désinformation sur X », Le Figaro, le 10 avril 2024, [en ligne :] https://www.lefigaro.fr/international/le-combat-entre-un-juge-bresilien-et-elon-musk-a-propos-de-la-desinformation-sur-x-20240410, consulté le 24 août 2024.

[96] Le Monde avec AFP, « Au Brésil, le réseau social X devient inaccessible après une décision de suspension d'un juge de la Cour suprême », Le Monde, le 10 août 2024, [en ligne :] https://www.lemonde.fr/pixels/article/2024/08/30/au-bresil-un-juge-de-la-cour-supreme-ordonne-de-suspendre-le-reseau-social-x_6299835_4408996.html, consulté le 25 août 2024.

[97] Pezet J., « En quoi consiste le contrôle judiciaire de Pavel Dourov, patron de Telegram, interdit de quitter la France ? », Libération, le 29 août 2024, [en ligne :] https://www.liberation.fr/checknews/en-quoi-consiste-le-controle-judiciaire-de-pavel-durov-patron-de-telegram-interdit-de-quitter-la-france-20240829_WZSV77N2LVBXDFSASEUOVT6LRE, consulté le 3 septembre 2024.

[98] Smyrnaios N. et Papaevangelou C., « Guerre en Ukraine : les plateformes numériques rattrapées par la géopolitique », La revue des médias (INA), le 12 avril 2022, [en ligne :] https://larevuedesmedias.ina.fr/guerre-ukraine-plateformes-numeriques-gafam-deplateformisation-interdiction, consulté le 25 août 2024.

[99] Arrêt du Tribunal dans l'affaire T-125/22 | RT France/Conseil, « Le Tribunal, en grande chambre, rejette la demande de RT France d'annuler les actes du Conseil, adoptés à la suite du déclenchement de la Guerre en Ukraine, lui interdisant temporairement de diffuser des contenus », Cour de Justice de l'Union Européenne, le 27 juillet 2022, [en ligne :] https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-07/cp220132fr.pdf, consulté le 25 août 2024.

[100] La rédaction de la RTBF avec Agence, « Le Centre pour la Cybersécurité Belgique met en garde les entreprises belges contre une attaque des serveurs de Microsoft », RTBF, le 21 mars 2021, [en ligne :] https://www.rtbf.be/article/le-centre-pour-la-cybersecurite-belgique-met-en-garde-les-entreprises-belges-contre-une-attaque-des-serveurs-de-microsoft-10715113 , consulté le 26 août 2024.

[101] Manceau G., « Piratage massif de ChatGPT : comment vérifier si votre compte est compromis », 01net, le 21 juin 2023, [en ligne :] https://www.01net.com/actualites/piratage-massif-de-chatgpt-comment-verifier-si-votre-compte-est-compromis.html, consulté le 24 août 2024.

[102] Van der Ven M., « Des chercheurs découvrent plus de 5.000 courriels Microsoft usurpés », DataNews-Le Vif, 9 octobre 2024, [en ligne :] https://datanews.levif.be/actualite/securite/failles/des-chercheurs-decouvrent-plus-de-5-000-courriels-microsoft-usurpes, consulté le 10 octobre 2024.

[103] Stroobant J-P., « Aux Pays-Bas, la police victime d'un gigantesque vol de données », Le Monde, le 4 octobre 2024, [en ligne :] https://www.lemonde.fr/pixels/article/2024/10/04/aux-pays-bas-la-police-victime-d-un-gigantesque-vol-de-donnees_6343839_4408996.html, consulté le 10 octobre 2024.

[104] Check Point Research, « Check Point Research Reveals Q2 2024 Brand Phishing Trends: Microsoft Tops List While New Enntes Signal Shifting Threat Landscape », Check Point Software Technologies Ltd., le 24 juillet 2024, [en ligne :] https://blog.checkpoint.com/research/check-point-research-reveals-q2-2024-brand-phishing-trends-microsoft-tops-list-while-new-entries-signal-shifting-threat-landscape, consulté le 10 octobre 2024.

[105] Reynier V., « L'interconnexion des logiciels nous rend "plus vulnérables", selon un expert », Euronews, le 17 juillet 2024, [en ligne :] https://fr.euronews.com/next/2024/07/19/linterconnexion-des-logiciels-nous-rend-plus-vulnerables-selon-un-expert, consulté le 23 août 2024.

[106] Richman B., Fukuyama F. et Goel A., « How to Save Democracy From Technology », Foreign Affairs, le 24 novembre 2020, [en ligne :] https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy-technology, consulté le 2 septembre 2024.

[107] Couturier B., « Les GAFAM, une menace pour la démocratie ? », France Culture, le 25 novembre 2020, [en ligne :] https://www.radiofrance.fr/franceculture/podcasts/le-tour-du-monde-des-idees/les-gafam-une-menace-pour-la-democratie-5676358, consulté le 2 septembre 2024.

[108] *Ibid.*

[109] Jolly J., « EU lawmakers ask Jeff Bezos whether Amazon spies on politicians », The Guardian, le 7 octobre 2020, [en ligne :] https://www.theguardian.com/technology/2020/oct/07/eu-lawmakers-ask-jeff-bezos-whether-amazon-spies-on-politicians, consulté le 25 août 2024.

[110] Comme Tony Belpaeme : professeur en IA et Robotique à l'Université de Gent ; Tom Lenaerts : spécialiste de l'IA, vice-président du département d'informatique de l'ULB, Président de l'Association Benelux pour l'IA et expert au sein du Global Partnership on AI, Georg Riekeles Directeur associé du European Policy Centre, Risto Uuk : Responsable de recherche pour l'UE au Future of Life Institute ; Cristina Vanberghen : Professeur Dr., EUI et Commission européenne, Reconnue par le Service européen pour l'action extérieure (SEAE) pour son rôle dans l'avancement de la diplomatie numérique dans le cadre du G20 et du G7, en particulier pour ses efforts dans la promotion de l'agenda numérique et cybernétique de l'UE en collaboration avec les pays partenaires ; Lode Lauwaert : Professeur de Philosophie de la technologie, KU Leuven ; Frederic Heymans : Chercheur au Knowledge Centre Data & Society ; Gianluca Bontempi : Professeur à l'ULB et fondateur du ULB Machine Learning Group …

[111] Open Letter of experts, « Disrupting the Deepfake Supply Chain », OpenLetter.net, le 21 février 2024, [en ligne :] https://openletter.net/l/disrupting-deepfakes, consulté le 26 août 2024

[112] Voir dans ce cahier du numérique de Citoyenneté & Participation, Courteille P., « Deepfakes, le mensonge à l'ère de l'intelligence artificielle ».

[113] Selon une enquête menée par l'organisation sectorielle Febelfin, en collaboration avec le bureau d'études Indiville.

[114] Febelfin, « Chiffres 2023 : "Phishing et autres arnaques en vue" », Febelfin, juin 2024, [en ligne :] https://febelfin.be/media/pages/publicaties/2024/phishing-en-andere-kapers-op-de-kust/11470d102f-1718872012/storytelling_phishing_fr_final.pdf, consulté le 26 août 2024.

[115] Courteille P., « Fakeland, un nouvel et obscur continent », Citoyenneté & participation, Étude n°31, avril 2020 [en ligne :] https://www.cpcp.be/publications/fakeland.

[116] Documentaire de Sabine Pirolt et Matteo Born, « Hackers, comment ils violent notre intimité », 2023, diffusé sur Tipik le 9 janvier 2024.

[117] Documentaire de Peter Porta, Le piège du clic, diffusé dans l'émission Doc Shot sur la Une, RTBF, le 13 juin 2024 à 22h35.

[118] Documentaire de Sabine Pirolt et Matteo Born, *op. cit.*

[119] Steffens E., « Près de la moitié des filles de 15 à 25 ans ont déjà reçu un "dickpic" non désiré », VRTnws, le 7 février 2023, [en ligne :] https://www.vrt.be/vrtnws/fr/2023/02/07/pres-de-la-moitie-des-filles-de-15-a-25-ans-ont-deja-recu-un-di, consulté le 26 août 2024.

[120] Huttin C., « Harcèlement scolaire : 280 écoles sont invitées à lutter contre ce "fléau" », Le Soir, le 10 février 2024, [en ligne :] https://www.lesoir.be/567489/article/2024-02-10/harcelement-scolaire-280-ecoles-sont-invitees-lutter-contre-ce-fleau, consulté le 28 août 2024.

[121] Hildesheim M., « Une dizaine de jeunes filles élèves du collège Saint-Remacle de Stavelot victimes de deepfakes », Rtbf Info, le 21 juin 2024, [en ligne :] https://www.rtbf.be/article/une-dizaine-de-jeunes-filles-eleves-du-college-saint-remacle-de-stavelot-victimes-de-deepfakes-11392755, consulté le 3 septembre 2024.

[122] Courteille P., « Fakeland, un nouvel et obscur continent », *op. cit.*

[123] Gobeil, « La désinformation à l'étranger s'abreuve de contenus produits au Canada », Radio Canada, le 15 mars 2021, [en ligne :] https://ici.radio-canada.ca/nouvelle/1776786/covid-desinformation-chine-russie-etats-unis-canada-global-research, consulté le 3 septembre 2024.

[124] CBC News, « COVID-19 : la Russie et la Chine seraient à l'origine de la vague de désinformation », Radio Canada, le 29 mai 2020, [en ligne :] https://ici.radio-canada.ca/nouvelle/1707527/covid-19-la-russie-et-la-chine-seraient-a-lorigine-de-la-vague-de-desinformation, consulté le 3 septembre 2024.

[125] Belga, « Les fake news influencent notre jugement et notre mémoire », RTBF, le 17 avril 2018, [en ligne :] https://www.rtbf.be/article/les-fake news-influencent-notre-jugement-et-notre-memoire-9894974, consulté le 3 septembre 2024.

[126] RTL Info et Parmentier L., « Des élus belges cyberattaqués par la Chine condamnent publiquement : "Il est temps de défier Pékin" », RTL Info, le 29 avril 2024, [en ligne :] https://www.rtl.be/actu/belgique/politique/des-elus-belges-cyberattaques-par-la-chine-condamnent-publiquement-il-est-temps/2024-04-29/article/663921, consulté le 4 septembre 2024.

[127] RTBF Info, « Cyberviolences : des femmes politiques témoignent », RTBF, le 12 octobre 2022, [en ligne :] https://www.rtbf.be/article/cyberviolences-des-femmes-politiques-temoignent-10080151, consulté le 4 septembre 2024.

[128] *Ibid.*

[129] Belga, « Les jeunes femmes politiques, cyberharcelées », Rtbf Info, le 20 mai 2019, [en ligne :] https://www.rtbf.be/article/les-jeunes-femmes-politiques-cyberharcelees-10225196, consulté le 4 septembre 2024.

[130] Constantinidis A., « État de la liberté de la presse en Belgique. Éclairages sur le classement 2022 de Reporters sans frontières », Citoyenneté & Participation, Analyse n°469, Janvier 2023, [en ligne :] https://www.cpcp.be/wp-content/uploads/2023/01/liberte-presse.pdf.

[131] Gebruers P., « Frapper un journaliste », MEDORT, le 04 mars 2021 https://medor.coop/magazines/medor-n22-printemps-2021/frapper-un-journaliste-menace-censure-harcelement/?full=1, consulté le 5 septembre 2024.

[132] *Ibid.*

[133] *Ibid.*

[134] Unesco, « Enquête mondiale de l'UNESCO sur la violence en ligne contre les femmes journalistes », Unesco, le 15 décembre 2020, [en ligne :] https://www.unesco.org/fr/articles/enquete-mondiale-de-lunesco-sur-la-violence-en-ligne-contre-les-femmes-journalistes, consulté le 4 septembre.

[135] Centre belge de ressource en Éducation aux Médias, association d'Éducation permanente et agence de communication.

[136] Monin J., « Le projet Pegasus : un logiciel espion utilisé par des États pour cibler des politiques, des journalistes, des avocats... y compris des Français », France info, le 18 juillet 2021, [en ligne :] https://www.francetvinfo.fr/monde/proche-orient/disparition-d-un-journaliste-saoudien/enquete-le-projet-pegasus-un-logiciel-espion-utilise-par-des-etats-pour-cibler-des-politiques-des-journalistes-des-avocats-y-compris-des-francais_4707199.html, consulté le 1 septembre 2024.

[137] Renon D., « L'État fédéral allemand victime d'une cyberattaque », Courrier International, le 1 mars 2018, [en ligne :] https://www.courrierinternational.com/article/letat-federal-allemand-victime-dune-cyberattaque, consulté le 26 août 2024.

[138] L. Th., « Demeyer : "On n'a pas payé la rançon après la cyberattaque dont la Ville de Liège a été victime" », L'Avenir, le 8 juillet 2021, [en ligne :] https://www.lavenir.net/regions/liege/liege/2021/07/08/demeyer-on-na-pas-paye-la-rancon-apres-la-cyberattaque-dont-la-ville-de-liege-a-ete-victime-XCKV6NXYGJGW7H3FTIOQ2CASPQ, consulté le 10 août 2024.

[139] Noulet J-F., « "On est attaqué de toute part" : voici le contexte qui justifie la création d'une composante "Cyber" à la Défense belge », RTBF Info, 19 octobre 2022, [en ligne :] https://www.rtbf.be/article/on-est-attaque-de-toute-part-voici-le-contexte-qui-justifie-la-creation-dune-composante-cyber-a-la-defense-belge-11088541, consulté le 21 août 2024.

[140] Lekeu G., « La commune belge de Maldegem victime d'un piratage massif : les hackers exigent 200.000 $ », l'Avenir, 8 août 2022, [en ligne :] https://www.lavenir.net/actu/conso/multimedia/2022/08/08/la-commune-belge-de-maldegem-victime-dun-piratage-massif-les-hackers-exigent-200000-JGWJX-HFPXNCTDBMEDORQ5QYGN4, consulté le 21 août 2024.

[141] DDoS, c'est-à-dire « par dénis de service distribué », distributed denial of service, qui consiste à inonder les serveurs de requêtes pour les rendre inopérants.

[142] La rédaction de Rtbf Info et Belga, « Des sites de services publics piratés ce dimanche : une nouvelle attaque de type DDOS », Rtbf, le 16 octobre 2023, [en ligne :] https://www.rtbf.be/article/des-sites-de-services-publics-pirates-ce-dimanche-une-nouvelle-attaque-de-type-ddos-11272516, consulté le 23 août 2024.

[143] La rédaction de Data News, « Troisième jour consécutif de cyberattaques contre des sites de communes belges », Data News, le 9 octobre 2024, [en ligne :] https://datanews.levif.be/actualite/securite/cybercrime/troisieme-jour-consecutif-de-cyberattaques-contre-des-sites-de-communes-belges, 10 octobre 2024.

[144] Entretien avec Elise Degrave, « Le droit de contrôler », IMag, n° 371 - Mars-Avril 2024.

[145] Chiffres disponibles sur le site de l'IBPT, par année et en ligne, sur https://www.ibpt.be/operateurs/enquetes, consulté le 3 août 2024.

[146] Entretien avec Elise Degrave, « Le droit de contrôler », *op. cit.*

[147] Gillet E., « Numérisation du recrutement et de l'orientation », Citoyenneté & Participation, analyse n°472, juin 2023, [en ligne :] https://www.cpcp.be/publications/numerisation-recrutement/, consulté le 30 juin 2023.

[148] Essyad A., « La gravité de la cyberattaque de la commune de Rolle sous-estimée par les autorités », RTS, le 25 août 2021, [en ligne :] https://www.rts.ch/info/regions/vaud/12442317-la-gravite-de-la-cyberattaque-de-la-commune-de-rolle-sousestimee-par-les-autorites.html, consulté le 25 août 2024.

[149] La rédaction de BBC, « Comment un pirate informatique adolescent est devenu l'un des criminels les plus recherchés d'Europe », BBC, le 13 mai 2024, [en ligne :] https://www.bbc.com/afrique/articles/cpwg3e43qzno, consulté le 22 août 2024.

[150] *Ibid.*

[151] La rédaction du Courrier International, « Cyberattaque. Un pirate informatique tente d'empoisonner l'eau d'une ville en Floride », Courrier International, le 9 février 2021, [en ligne :] https://www.courrierinternational.com/article/cyberattaque-un-pirate-informatique-tente-dempoisonner-leau-dune-ville-en-floride, consulté le 27 juillet 2024.

[152] Lyngaas S., « Federal investigators confirm multiple US water utilities hit by hackersé », CNN Politics, le 1 décembre 2023, [en ligne :] https://edition.cnn.com/2023/12/01/politics/us-water-utilities-hack/index.html, consulté le 27 juillet 2024.

[153] Deschamps T., « Inédit en Europe : la Belgique instaure une protection pour les hackers éthiques, sous certaines conditions », Rtbf, le 23 février 2023, [en ligne :] https://www.rtbf.be/article/inedit-en-europe-la-belgique-instaure-une-protection-pour-les-hackers-ethiques-sous-certaines-conditions-11156779, consulté le 27 juillet 2024.

[154] Clasen A., « Cyberdéfense active : l'UE envisage le recours au « hacking de représailles », Euractiv, le 21 novembre 2023, [en ligne :] https://www.euractiv.fr/section/cybersecurite/news/cyberdefense-active-lue-envisage-le-recours-au-hacking-de-represailles, consulté le 28 juillet 2024.

[155] Cert-Fr est le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques en France.

[156] Bulletin d'alerte du Cert-Fr, « Recrudescence d'activité Emotet en France », Cert-Fr, le 7 septembre 2020, [en ligne :] https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-019, consulté le 28 juillet 2024.

[157] Reynaud F. et Clairouin O., « Avortement : aux États-Unis, les géants du numérique face au danger lié aux données personnelles », Le Monde, le 27 juin 2022, [en ligne :] https://www.lemonde.fr/pixels/article/2022/06/27/avortement-aux-etats-unis-les-geants-du-numerique-face-au-danger-lies-aux-donnees-personnelles_6132221_4408996.html, consulté le 19 août 2024.

[158] Les journalistes ont passé au crible les résultats du logiciel Compas, de la société Northpointe, très utilisé. En comparant les scores de risque de récidive attribués par le programme et les cas de récidive réels – en excluant les personnes incarcérées – sur l'ensemble d'un comté pendant deux ans, les enquêteurs ont établi une série de statistiques sur l'efficacité du logiciel.

[159] La rédaction du Monde, « L'échec des logiciels de prévention des risques de récidive aux Etats-Unis », Le Monde, le 24 mai 2016, [en ligne :] https://www.lemonde.fr/pixels/article/2016/05/24/aux-etats-unis-l-echec-des-algorithmes-qui-cherchent-a-predire-le-risque-de-recidive_4925242_4408996.html, consulté le 24 août 2024.

[160] Sugy P., « À cause de ChatGPT, un avocat américain cite des arrêts… qui n'ont jamais existé », Le Figaro International, le 30 mai 2023, [en ligne :] https://www.lefigaro.fr/sciences/a-cause-de-chatgpt-un-avocat-americain-cite-des-arrets-qui-n-ont-jamais-existe-20230529, consulté le 25 août 2024.

[161] Laloux P., « Comment l'Etat joue avec les données des Belges », Le Soir, 11 fécrier 2021, [en ligne :] https://www.lesoir.be/354396/article/2021-02-11/comment-letat-joue-avec-les-donnees-des-belges, consulté le 8 mai 2024.

[162] Entretien avec Elise Degrave, « Le droit de contrôler », dans IMag, n° 371 - Mars-Avril 2024

[163] *Ibid.*

[164] Communiqué de presse de la Commission européenne, « Entrée en vigueur du règlement européen sur les données, mettant en place de nouvelles règles pour une économie fondée sur les données équitable et innovante », Commission européenne, le 11 janvier 2024, [en ligne :] https://digital-strategy.ec.europa.eu/fr/news/european-data-act-enters-force-putting-place-new-rules-fair-and-innovative-data-economy, consulté le 8 mai 2024.

[165] Bascou S., « Avec le Data Governance Act, un nouveau règlement européen, vous pourriez choisir de davantage partager vos données », 01net, le 5 novembre 2023, [en ligne :] https://www.01net.com/actualites/data-governance-act-la-nouvelle-loi-europeenne-sur-les-donnees-va-t-elle-faire-emerger-un-marche-europeen.html, consulté le 8 mai 2024.

[166] AFP, « Atteinte aux droits d'auteur: le New York Times attaque en justice OpenAI, l'entreprise créatrice de Chat GPT », RTBF, le 28 décembre 2023, [en ligne :] https://www.rtbf.be/article/atteinte-aux-droits-d-auteur-le-new-york-times-attaque-en-justice-openai-l-entreprise-creatrice-de-chat-gpt-11306144, consulté le 16 juillet 2024.

[167] Ziegler J., « Cyberdémocratie et démocratie participative », Open Edition Books, le 5 mai 2017, [en ligne :] https://books.openedition.org/pupvd/2782, consulté 19 juillet 2024.

[168] *Ibid.*

[169] Boudet A., « Les théories du complot attirent les jeunes, surtout ceux qui s'informent sur les réseaux sociaux », Huffpost, le 12 janvier 2023, [en ligne :] https://www.huffingtonpost.fr/science/article/les-theories-du-complot-attirent-les-jeunes-surtout-ceux-qui-s-informent-sur-les-reseaux-sociaux_212673.html, consulté le 27 août 2024.

[170] Flichy P., « Internet et le débat démocratique », Cairn Info, janvier 2008, [en ligne :] https://shs.cairn.info/revue-reseaux1-2008-4-page-159?lang=fr&contenu=article, consulté le 3 septembre 2024.

[171] Le RGPD et ses acceptations de cookies sont même vus comme des règles pompeuses des pouvoirs, voire une entrave à leur liberté, le discours classique des plateformes.

[172] Le quishing est une variante du phishing utilisant des QR codes.

[173] Use-After-Free (UAF) est une vulnérabilité primitive de corruption de la mémoire qui continue à représenter une menace importante pour tous les types de logiciels, des systèmes d'exploitation aux logiciels d'application. Cette faille de sécurité critique se produit lorsqu'un composant d'application tente d'accéder à des données dans une adresse mémoire qui a déjà été libérée, d'où son nom : use-after-free (utilisation après libération).

[174] Des courtiers en données personnelles.

[175] Ses paramétrages privés.

[176] Le back-up consiste à créer des copies de sécurité de ses données vitales et à les stocker en toute sécurité.

[177] « Le temps important consacré aux activités sur écrans sollicite fortement la vision de près, au même titre que la faible exposition à la lumière naturelle, du fait de la diminution des activités en extérieur et de l'allongement de la durée des études qui favorisent le travail intensif de près », explique M. Assouly, fondateur de l'IEMP, l'Institut d'éducation médicale et de prévention, sis à Lyon. Dans « L'emprise des écrans sur les enfants, vecteur grandissant de la "pandémie" de myopie », Guillaume Delacroix, 25 juin 2022

[178] Llach L., « “Cela vous marque à vie” : des modérateurs traumatisés par des vidéos violentes poursuivent Meta », Euronews, le 19 octobre 2023, [en ligne :] https://fr.euronews.com/2023/10/19/cela-vous-marque-a-vie-des-moderateurs-traumatises-par-des-videos-violentes-poursuivent-me, consulté le 7 juillet 2024.

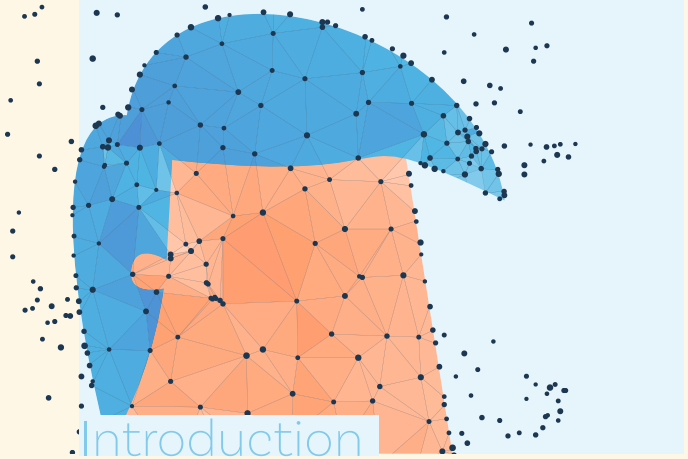
[179] Entretien avec Elise Degrave, « Le droit de contrôler », IMag, n° 371 - Mars-Avril 2024.

Edgar Gillet est diplômé de Sciences Po Strasbourg en affaires européennes, anciennement chargé de recherche dans la thématique Médias & Actions citoyennes chez Citoyenneté & Participation.

Numérisation du recrutement et de l'orientation

Promesses et conséquences des algorithmes

Edgar Gillet



Introduction

La numérisation du monde s'observe à toutes les échelles de la société. Un aspect central de la vie contemporaine offre même un point de vue privilégié sur ses conséquences : le travail. Plus précisément, les champs de l'orientation et du recrutement, en se situant à l'interface entre la vie privée et le monde de l'entreprise concentrent les enjeux liés au numérique. En effet, la mise en place en entreprise de logiciels intégrés, gérant la recherche et l'embauche de nouveaux employés, automatise aujourd'hui des processus assurés autrefois par des êtres humains, pour des êtres humains. Ces nouveaux outils permettent ce faisant, un passage à l'échelle supérieure considérable. Selon le logiciel choisi, les algorithmes trient et analysent plusieurs milliers de candidats en quelques secondes. Plus loin encore, certains algorithmes dits de recrutements prédictifs, débusquent et suggèrent les candidats les plus proches des critères des employeurs, remplaçant presque les professionnels du domaine.

Dès lors, dans quelle mesure ces nouveaux outils influencent-ils les pratiques en lien avec le recrutement au sein des organisations ? Quels sont leurs apports et leurs conséquences, tant pour les professionnels du recrutement, que pour les recrutés ? Et ces apports se limitent-ils à la seule entreprise ? Portés par des discours de promotion vantant leur objectivité et gains en productivité, l'origine et le choix de ces nouveaux outils soulèvent plusieurs interrogations liées au rôle de ceux-ci dans nos vies professionnelles. C'est pourquoi nous proposerons dans cette analyse, un panorama critique des outils numériques de recrutement et de formations.

Pour traiter de la question, nous reviendrons d'abord aux fondements des disciplines du recrutement et de l'orientation, la manière dont elles se sont construites historiquement ainsi que les courants marquants qui les ont façonnées. On observera ce faisant, à rebours d'une idée d'outils neutres, la transposition aujourd'hui, dans les nouveaux outils numériques, de philosophies, dont les algorithmes de recrutement sont les dépositaires. Nous observerons ensuite comment le fonctionnement de ces nouveaux outils, vient, en situation s'hybrider avec les pratiques antérieures des recruteurs sans pour autant normaliser et harmoniser celles-ci. Nous verrons aussi, comment le déploiement et la maîtrise des outils numériques croisent des stratégies de présentation de soi, propres au champ du recrutement et participant de leur légitimation, et ce alors qu'ils sont porteurs de biais techniques. Nous aborderons enfin, les implications plus générales, du déploiement d'outils numériques sur la formation initiale et continue.

1. Aux origines de l'orientation professionnelle matching et life design : nouveaux outils, vieux modèles.

a. Les modèles du matching et du life design

L'orientation et le recrutement dépendent aujourd'hui de modèles plus anciens, qui se sont construits historiquement et dont on retrouve la philosophie au cœur des outils actuels. Théorisé dès le début du XX[e] siècle le modèle dit du « matching »[1] (modèle par correspondance, en français) s'impose à partir des années 1960 comme approche majoritaire dans le champ de l'orientation professionnelle. Promue par les conseillers en orientation, elle impulse à cette époque la prise en compte des traits individuels (centres d'intérêts, personnalités) dans la recherche et l'assignation d'un emploi à un candidat[2]. Elle remplace ce faisant une orientation centrée auparavant sur les secteurs en tension, l'état du marché et les compétences techniques[3]. À ces critères, le matching propose de superposer des données personnelles, pour correspondre à une grille de métiers compatibles. La popularisation de cette approche entraîne progressivement les futurs employés vers un choix de carrière en fonction de leurs inclinations, loisirs et affinités. Surtout, les candidats doivent désormais s'impliquer activement dans la formulation de leurs projets. À charge pour ces derniers en effet de formuler clairement leurs intérêts et penchants personnels pour trouver le métier en rapport avec

leurs aspirations. Les employés deviennent donc, à l'époque, acteurs de leur propre carrière, dans le sens où ils deviennent responsables des choix en rapport et des directions que celle-ci prend. On assiste de fait à un « *basculement de la responsabilité de la gestion des cheminements professionnels vers les individus […]. La mobilité des travailleurs est renforcée et elle se bâtit sur une attitude individuelle de liberté, d'autodétermination et de choix fondés sur les valeurs personnelles* »[4].

Le début des années 2000 voit par la suite, l'émergence du concept de « life design »[5] dans le champ de la recherche en orientation. Cette approche propose alors un modèle à destination des conseillers en orientation pour soutenir les candidats dans « *la structuration de leur identité narrative* »[6], la mise en récit de leurs besoins et aspirations en lien avec le travail. Surtout, le life design promeut une certaine souplesse chez les candidats pour « *développer les ressources nécessaires et répondre aux incertitudes inhérentes à tout parcours professionnel au xxie siècle* »[7].

Ce tournant dans les approches de l'orientation professionnelles marque alors une responsabilisation de l'individu dans la gestion de sa carrière. En effet, se concentrer sur les caractéristiques personnelles des travailleurs, fait porter la responsabilité de sa carrière au seul individu, en mettant de côté les difficultés d'ordre structurel, comme un licenciement ou une crise économique[8]. Il lui revient alors à lui seul de travailler sur des causes internes, afin de concrétiser son projet professionnel. Pourtant, les individus évoluent dans un environnement social, économique et politique, difficiles à séparer de leur parcours d'orientation. On parle alors de pouvoir d'action limité (bounded agency)[9] : l'individu possède « *une certaine autonomie et un pouvoir décisionnel, mais celui-ci s'exerce dans un environnement aux opportunités limitées* »[10].

b. Le passage au numérique dans le recrutement, Monkey Tie et l'"optimized hiring"

C'est dans ce contexte, qu'on observe, à la même époque le déploiement de nouveaux outils numériques dans le champ des ressources humaines, qui, on le verra, renforcent cette individualisation des travailleurs devant leur destin professionnel. À l'instar des conseillers en orientation des années 1960, les créateurs de ces nouveaux outils sont des professionnels du recrutement et du conseil en orientation, se réclamant de différents courants dans leurs champs respectifs. Ils se saisissent au tournant des années 2010 et du boom de l'Internet 2.0, de nouvelles possibilités techniques, se positionnant alors sur le marché du recrutement. Ils participent en cela, à la construction d'un nouvel aspect de leurs professions, en même temps qu'à la normalisation des outils qui en découlent. Parmi eux, Monkey Tie est une plateforme en ligne française qui propose des outils pour le recrutement et le développement professionnel basés sur l'intelligence artificielle. Créée en 2012, la plateforme utilise des algorithmes qui font correspondre les compétences et les préférences des candidats avec des offres d'emploi. Elle se propose aussi d'identifier les lacunes en compétences des employés, pour offrir des plans de formation personnalisés[11]. Un de ses fondateurs, Jérémy Lamri, présente l'entreprise de cette manière :

> « J'ai fondé Monkey Tie en 2012 afin d'aider les entreprises à identifier et capitaliser les talents grâce au matching affinitaire. Le matching affinitaire est un concept qui vise à prendre en compte, en plus des compétences techniques, les « softs skills », c'est-à-dire la personnalité et les moteurs de motivations.[12]

Monkey Tie illustre, par sa notoriété, l'engouement qu'a pu incarner son projet au début des années 2010. Start-up au départ, elle a bénéficié d'une certaine couverture médiatique à son lancement grâce à des levées de fonds réussies[13], avant de décrocher plusieurs contrats pour l'administration française[14]. Surtout, Jérémy Lamri est un professionnel reconnu dans le champ du recrutement et des ressources humaines[15]. Il participe à la rédaction d'ouvrages de recherche sur les ressources humaines[16], et s'illustre particulièrement par son investissement dans des laboratoires d'innovation[17]. Le parcours et le fonctionnement de Monkey Tie viennent donc percuter l'illusion d'un outil neutre[18], pourtant au cœur des stratégies marketing promouvant la plateforme. Sous le vocable de matching affinitaire, on retrouve en effet la philosophie du matching du xxe siècle, transposée dans un outil numérique. Accorder employeurs et candidats sur la base des motivations et affinités personnelles des candidats, en plus de leurs compétences techniques et expériences professionnelles, reprend de fait une approche historique de l'orientation. Surtout, elle en reprend les implications, et individualise également les employés dans leur parcours professionnel. Elle contribue ce faisant à invisibiliser des circonstances structurelles ou extérieures qui échappent aux individus, mais influencent pourtant bel et bien leur carrière.

Plus loin encore, l'emploi de l'expression « soft skills » par Jérémy Lamri permet de rapprocher Monkey Tie du mouvement dit de l'« optimized hiring » (« recrutement optimisé » en français). Également présent dans les stratégies de marketing, le vocable d'« optimized hiring » concerne les entreprises ayant recours à des processus de recrutement testant les candidats sur des critères non conventionnels[19]. Au lieu d'évaluer les candidats sur la base de leurs qualifications techniques, de leurs diplômes et d'entretiens personnels, les organisations leur font passer des tests de

personnalité (parfois sous la forme de jeux[20]), avant de les sélectionner selon des corrélations statistiques entre la manière dont un candidat répond à certaines questions, et l'impact qu'elles pourraient avoir sur sa performance au travail. Souvent mise en avant, l'approche allie systématiquement ses processus à des outils numériques, producteurs de données. Les plateformes qui s'en réclament (Hirevue[21], Pyremetrics[22]…) multiplient de fait les tests, simulations et mises en situation. Dès lors, la numérisation des pratiques du recrutement incarne-t-elle une réponse efficace aux problématiques de gestion des ressources humaines de l'entreprise (acquisition des talents, suivi des carrières) ou suit-elle une économie des données ?

2. Le passage au numérique : entre appropriation, biais et stratégies d'acteurs

a. Fonctionnement des outils

Pour pouvoir être soumis aux algorithmes des plateformes de recrutement, les profils des candidats sont de fait réduits à des données quantifiables et objectives, telles que leurs antécédents académiques et professionnels, leurs compétences techniques ou leurs résultats à des tests standardisés[23]. Or, partir de 2010, l'accès à de grandes quantités de données, combiné à la puissance de traitement des ordinateurs, accessibles à distance et à la demande, marque l'avènement d'algorithmes plus pointus, capables de choix autonomes et se substituant à un raisonnement humain : l'intelligence artificielle[24]. Autoapprenants, ces algorithmes détectent automatiquement les tendances qui ressortent d'un ensemble de données, et peuvent alors être utilisés pour faire correspondre candidats et entreprises. Nouveau paradigme autant qu'argument marketing, l'irruption du principe d'intelligence artificielle vient alors bouleverser des pratiques de recrutement déjà en mutation. Car avant la généralisation d'algorithmes autonomes, le travail en contexte numérique impliquait déjà le recours à de nouveaux outils impulsant des changements de pratiques.

b. Hybridation et cohabitation des pratiques

Le premier d'entre eux, l'Applicant Tracking System (ATS) d'une entreprise, constitue une base de données privative reliée au site de l'entreprise et parfois à d'autres *job boards*[25]. L'ATS permet le suivi des offres et candidatures pour des postes au sein des organisations. En reliant davantage de prospects et différemment (sur les plateformes de recrutement, avec des entretiens différés ou à distance, etc.), il permet aux recruteurs de mettre au point d'importants ensembles de données analysables par des algorithmes. D'autres outils viennent s'y ajouter et permettent aussi d'archiver ces données ou de les manipuler de manière à se constituer, par exemple, des viviers de candidats. Le numérique permet également de multiplier les canaux de diffusion des annonces (sites de réseautage, d'emploi, etc.)[26]. Pourtant, les recruteurs, s'ils s'approprient ces nouveaux outils, le font aussi avec des usages plus anciens (comme les tableurs Excel), différant des pratiques de production de masse soutenues par les industriels des plateformes[27]. Dès lors, si les outils algorithmiques prennent le pas sur l'organisation du travail en contexte numérique, on continue d'observer leur hybridation et leur cohabitation avec des pratiques plus traditionnelles : les pratiques de recrutement ne dénotent alors pas d'une « normalisation absolue »[28]. Ainsi, s'ils décalquent parfois leurs pratiques sur les modes de calculs et de représentations portés par les plateformes, les recruteurs n'en conservent pas moins une pratique propre et personnalisée.

On observe d'ailleurs à ce titre un changement dans la relation recruteurs-recrutés. Car si les outils numériques formalisent et rendent objectifs les profils des candidats en les réduisant à des flux d'informations, ils créent en parallèle de nouvelles formes de relations, sur un ton plus conversationnel/informel, avec une attention accrue portée au candidat[29]. Dans le flot des candidatures et de la recherche de talents, les recruteurs doivent en effet se démarquer pour convaincre leurs prospects, sans donner l'impression d'une sollicitation peu pertinente ou désincarnée[30]. Les compétences et les usages effectifs montrent de fait que les outils numériques ne modifient pas complètement les pratiques des recruteurs, même si les algorithmes et les *architextes*[31] standardisent et automatisent les modes de collecte et de traitement des données.

c. Stratégies d'acteurs

Pour les recruteurs, les outils numériques consolident un positionnement particulier : leur maîtrise permet de préserver un territoire professionnel dans les jeux entre groupes professionnels[32]. La maîtrise des outils numériques, la « littératie numérique » devient en effet un argument dans la manière de se présenter et de présenter son travail. Le recours au numérique s'analyse même comme une stratégie d'acteur dans les rapports de force et de légitimation des « bonnes pratiques » entre professionnels des RH[33]. Plus loin encore, Jérémy Lamri, dans un entretien à une

revue RH consacrée à l'IA, estime en parlant de l'intelligence artificielle, qu'elle appelle à « *identifier, en interne et en externe, les personnes qui pourront comprendre et porter ce changement* [34] » au sein des entreprises, afin « *de demeurer performant professionnellement* » [35]. La disparition des tâches parasites que permettrait la maîtrise de ces outils, ainsi que l'accès instantané et illimité à l'information, induiraient selon lui en effet, que les professionnels du recrutement poursuivent un apprentissage continu tout au long de leurs carrières [36]. Et se fait ainsi, l'avocat d'une grande flexibilité, de la part des professionnels.

d. Biais et machines

Enfin, l'intelligence artificielle, elle, est présentée comme une assistance, à même d'alléger la charge de travail d'un recruteur. Le logiciel d'acquisition des talents peut, de fait, parcourir les CV et évaluer des candidats, avant d'éliminer rapidement la plupart d'entre eux du processus de recrutement. Ce matching automatique laisse au recruteur humain le loisir de se concentrer sur une tâche moins contraignante, à partir d'un vivier de candidats éligibles plus restreint [37]. Surtout, les candidats ne seraient alors sélectionnés sur la seule base de leurs compétences, sans biais humains [38]. Telle que défendue par ses tenants, la numérisation des pratiques de recrutement présenterait en effet une opportunité pour les entreprises de gagner, à la fois en productivité et en diversité. Or, l'architecture même des algorithmes fait que ces derniers peuvent reproduire des biais existants dans les données utilisées pour les mettre au point. Si les données utilisées au départ présentent par exemple, une sous-représentation de certaines populations, l'algorithme développe à son tour, des biais en rapport et privilégie un profil type [39]. Le processus d'apprentissage automatique des algorithmes requiert en effet que ceux-ci soient exposés à des données d'entraînement, à partir desquelles ils s'établissent. Or, nourrir un processus automatisé de données biaisées, produit des résultats faussés à leur tour [40]. Ainsi, si les profils idéaux de candidats qui nourrissent l'algorithme, contiennent, en soi plusieurs préjugés (« le leadership, un trait "masculin" »), alors ces préjugés seront reproduits dans les recommandations de recrutement. Surtout, si l'échantillon à partir duquel les outils de recrutement prédictif sont étalonnés, comprend moins de candidats d'un groupe donné, alors toute décision de recrutement en rapport désavantagera les candidats sous-représentés dans les données d'apprentissage.

Ajoutons à cela l'influence des caractéristiques sociodémographiques des programmeurs lors de la conception des algorithmes. Dominé par les hommes, le milieu des programmeurs informatiques apporte parfois aux algorithmes plusieurs biais au moment de leur conception. Les algorithmes de traitement du langage illustrent à ce niveau, plusieurs stéréotypes de genre. En usant des techniques de « prolongements de mots » (*word embedding*) qui repèrent les associations de mots [41], on observe par exemple une forte association entre le genre de mots apparemment neutres en anglais et leur occurrence : le mot « femme » est ainsi davantage associé aux mots « foyer, bibliothécaire » ; le mot « homme », aux mots « maestro, skipper, philosophe » [42]. Plusieurs articles de recherche mettent également en évidence, une proportion plus importante d'erreurs dans le domaine de la reconnaissance faciale, lors de la détection des expressions du visage de candidats au physique atypique. Le taux d'erreur pour la reconnaissance d'une expression peut ainsi varier de 1% pour un homme blanc à 35% pour une femme noire [43]. Or, la reconnaissance faciale (utilisée dans le recrutement, on l'a vu avec Hirevue) illustre particulièrement bien la fiabilité à géométrie variable de certains algorithmes. Comme l'expliquent Lacroux & Martin-Lacroux :

> Les programmeurs (aidés par des psychologues) associent certaines expressions faciales à des traits de personnalité, qui sont à leur tour associés à certaines capacités managériales. Or, la validité prédictive de ce genre d'inférence est un sujet très débattu. Les mécanismes à l'œuvre notamment le rôle des stéréotypes de genre et des théories implicites de la personnalité demeurent un sujet de controverse [...] Les travaux récents menés sur la reconnaissance faciale des émotions fondamentales (colère, angoisse...) viennent renforcer les doutes sur la possibilité d'une reconnaissance automatique en montrant que le décodage de ces émotions est culturellement dépendant : une même mimique faciale est interprétée différemment selon les cultures [44].

Le fonctionnement d'un mécanisme automatisé, « artificiel » donc, dans l'élaboration d'un choix culturel, a dès lors une probabilité plus importante de mal interpréter certains signaux. On retrouve ici une tension au cœur des discours de promotion du recrutement prédictif : vantés comme objectifs, certains de ses outils s'appuient pourtant sur des critères bien arbitraires.

Dans le domaine du recrutement, ces biais se retrouvent majoritairement à l'étape du sourcing (la recherche de candidats par les recruteurs). L'algorithme Talent Match de la plateforme LinkedIn utilise par exemple, quinze critères pour faire correspondre candidats et besoins des employeurs, basés sur leurs embauches passées [45]. Mécaniquement, les employeurs discriminants se voient proposer des candidats reflétant leurs choix précédents. Or, les biais liés aux données d'entraînement ou à la sélection, ne sont

pas uniquement un vecteur de discrimination sexiste ou raciste : ils ont pour principale caractéristique de cloner la population de salariés existante. On retrouve aussi des biais en phase de choix, qui viennent questionner de même l'importance grandissante des outils automatisés dans le recrutement. Car si les promoteurs des outils de recrutement prédictif arguent que la décision finale revient toujours à un humain, le choix des candidats peut-être fortement impacté par les algorithmes de recommandation. Plusieurs biais décisionnels liés à la présentation des solutions, comme l'effet de cadrage influencent ainsi les décisions. Classés par ordre de « compatiblité », les candidats qui apparaissent en premier bénéficient d'une très forte « surprime » liée à ce mode de présentation[46]. Enfin, un biais dit « d'automation » survient lorsque le recruteur donne un poids déterminant aux informations provenant de l'algorithme. Ainsi, la confiance envers l'algorithme en situation de prise de décision à risque, serait supérieure à celle accordée aux humains, sauf chez les professionnels expérimentés[47].Plusieurs pistes existent pourtant pour atténuer les effets des différents biais. Intégrer une part d'aléatoire dans la présentation des résultats au recruteur permet d'éviter les biais de présentation susceptibles d'influencer le choix final au profit des profils apparaissant en première position[48]. Rendre aveugles les systèmes face à certaines caractéristiques sociodémographiques comme le sexe ou l'origine. Limiter les mots-clés de recherche à des termes techniques n'éradique pourtant pas la possibilité, pour le recruteur, de s'appuyer sur des indices subtils permettant d'écarter certains types de candidature[49]. Surtout, bien qu'illégal, il est facile de se représenter un employeur discriminant qui userait de ces critères à mauvais escient. La littérature scientifique retient de fait une méthode efficace mais à double tranchant : redresser les bases d'apprentissage, dans le but d'avantager les catégories discriminées[50]. Contre les biais discriminatoires dans les données de simulation, réviser les résultats obtenus permet en effet de mettre à jour les données utilisées dans l'apprentissage de l'algorithme, et d'aller au-delà de quotas minimums de diversité pour proposer un modèle systématiquement inclusif, à rebours d'une population salariée normée[51].

3. Formation initiale et continue : philosophie et conséquences

Le déploiement des outils numériques de recrutement soulève enfin plusieurs questionnements liés à la formation initiale ou continue. Appliqués aux politiques de gestion des ressources humaines, les algorithmes permettent aux entreprises, une personnalisation accrue de la formation des employés et du contrôle de ceux-ci. En utilisant des données sur les intérêts et performances des travailleurs, les algorithmes adaptent par exemple, le contenu de leurs programmes de formation. Les employés peuvent alors suivre l'évolution de leur carrière plus efficacement, tandis que l'entreprise suit en direct le diagnostic de compétences de ses collaborateurs ainsi que… leur rentabilité[52]. MySkillCamp, par exemple, est une plateforme d'apprentissage en ligne, développée au Royaume-Uni et en Belgique pour offrir une formation personnalisée aux employés[53]. Les algorithmes de la plateforme analysent les compétences et les intérêts de chaque employé pour recommander du contenu de formation.

a. L'orientation numérique : Parcoursup

Cette approche des individus par les compétences rejoint, ici à nouveau, une vision du monde où l'employé est acteur (et seul en charge) de sa propre carrière. On observe d'ailleurs le même phénomène dans le domaine des études, à travers la numérisation de l'orientation. Mise en place en 2018, la plateforme en ligne pour la gestion en France des admissions dans l'enseignement supérieur, Parcoursup, incarne cette numérisation. Parcoursup permet aux lycéens et étudiants de formuler des vœux pour des formations (universités, écoles, etc.) avant de recevoir des réponses des établissements auxquels ils ont postulé[54]. Les étudiants doivent pour ce faire, saisir leur dossier scolaire complet, depuis l'entrée au lycée, avant de formuler des vœux pour les formations qui les intéressent[55]. Les établissements examinent ensuite les dossiers des candidats et formulent des propositions d'admission en fonction de leurs critères de sélection. Pensée pour renforcer « la transparence et l'équité »[56] à l'entrée des études, Parcoursup, en fonctionnant sur la rédaction systématique de projets d'orientation et en impliquant une connexion permanente pour suivre les propositions d'affectation, renforce dans les faits une responsabilisation-individualisation des candidats. La plateforme fonctionne pourtant à partir d'éléments liés aux algorithmes, sur lesquels les étudiants ne peuvent avoir prise. La plateforme implique par exemple que l'ensemble des formations universitaires aient recours à des algorithmes locaux pour classer leurs candidats[57]. L'algorithme d'affectation (proposant une place pour chaque candidat) fait aussi office « d'algorithme d'appel »[58] (pour des propositions simultanées aux candidats) en insérant au passage des candidats boursiers ou « de secteur », selon des taux définis par académies. Or ces algorithmes, mettent au centre de l'orienta-

tion ou de la formation continue les données personnelles des étudiants et employés. Traitées en même temps que produites par ces outils, elles sont indissociables de modèles économiques, marchandant ces données en les partageant avec des tiers, à même de les utiliser à leur tour pour influencer les choix de carrière des étudiants et des travailleurs (performances académiques, intérêts personnels, habitudes de navigation en ligne). C'est dans ce contexte d'ailleurs que certaines entreprises proposent un passeport numérique[59], qui unirait formation et carrière. Utilisé pour stocker des informations sur les certifications, les compétences et l'expérience professionnelle d'une personne, le passeport permettrait de trouver plus facilement des candidats qualifiés. Il offrirait également une opportunité pour les individus de démontrer leurs compétences de manière transparente et efficace.

Ces systèmes posent pourtant la question du rôle de l'école et des études dans une société : si elles doivent être conçues pour prioriser les compétences et les connaissances considérées comme les plus utiles aux employeurs, ou si un autre horizon leur est permis.

b. Explicabilité

Enfin et surtout, à l'instar du recrutement, le déploiement dans l'orientation d'algorithmes de sélection devrait avant tout garantir aux premiers concernés les moyens de comprendre ses implications. L'« explicabilité », un concept né avec l'IA, est ainsi un critère majeur de responsabilité juridique des processus liés à l'intelligence artificielle. Le livre blanc de l'Union européenne sur l'intelligence artificielle la place par exemple au centre des droits soudés à l'usage de l'IA. La législation française (Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique) impose elle, d'« *expliquer une décision administrative obtenue par un traitement automatique lorsque la personne physique concernée en fait la demande* ». Car l'opacité autour des choix impulsés par les machines ferait le lit de violences institutionnelles, elles aussi passées à l'échelle.

Conclusion

Vanté pour le renouvellement des pratiques qu'il induit, le déploiement du numérique dans l'entreprise passe par des outils standards qui ont évolué depuis le début de années 2000 vers des équations plus performantes, autonomes, et à même de simuler un raisonnement humain. Dans les champs du recrutement et de l'orientation, le déploiement de ces outils est porté par des discours de promotion de l'intelligence artificielle, mettant en avant des mécanismes, basés sur un raisonnement abstrait et objectif, et supposément dénués de biais humains.

Ces algorithmes sont pourtant loin d'être neutres. Depuis le modèle du matching des années 1960, qui vit pour la première fois accoler des facteurs indirectement liés au travail à la recherche de celui-ci, jusqu'au mouvement dit d'« optimized hiring » qui compile et inventorie les softs skills des candidats (intelligence relationnelle, capacités de communication, résolution de problèmes…) avant de les proposer aux recruteurs, les nouveaux outils numériques sont tributaires dans leurs champs respectifs de courants historiques. Leur conception porte en soi des choix d'approches, à rebours des discours de neutralité les promouvant. S'en saisir en contexte conduit de fait à de nouvelles pratiques. En organisation (entreprise, mais aussi association, administration…), le recrutement est en effet au carrefour de plusieurs compétences professionnelles, mêlant gestion des ressources humaines et communication. Or l'usage des outils numériques y apparaît tant comme une réponse à de nouvelles contraintes, qu'un usage valorisé par les recruteurs. Faisant avec des usages plus anciens, en même temps que de nouveaux processus, les recruteurs se représentent ainsi, pour certains, le numérique, comme une opportunité de créer de nouveaux types de médiation (approches informelles des candidats, recherche de la perle rare…) sans pour autant les uniformiser. Les nouvelles pratiques communicationnelles qui en découlent, éloignent même, pour ces promoteurs, un travail routinier et rigide, revivifiant l'attrait pour le métier. Cet apport de l'IA dans la pratique quotidienne du travail, pose dès lors la question de l'intérêt de l'apport technologique au travail. Celui-ci pourrait se mesurer par exemple, à l'aune de l'allégement des tâches pénibles qu'il permettrait. Le rapport français Villani sur l'intelligence artificielle, évoquait en 2018 à ce titre, l'idée d'un « indice de complémentarité » entre l'homme et la machine. L'indice distinguerait les complémentarités souhaitables, dites « capacitantes », révélant le potentiel humain, des modes de complémentarité néfastes créant de la souffrance au travail par une perte d'autonomie du salarié. Ce modèle, servirait alors d'aiguillon, de boussole au déploiement de davantage d'algorithmes prédictifs dans le monde du travail. Car les outils servent aujourd'hui à la légitimation de groupe de professionnels en passe, il semblerait, de s'imposer. Surtout, l'intelligence artificielle et l'architecture de tout outil numérique de recrutement portent en soi des biais. Sans parler « d'opinions intégrées à du code »[60], le recours à l'intelligence artificielle dans la gestion des ressources humaines implique donc de mettre à distance les discours de promotion et de se concentrer sur les conséquences très concrètes de celle-ci. L'une des promesses du recrutement prédictif propose par exemple de fournir clés en main le ou la candidate idéale à chaque organisation, en fonction de ses besoins. Pourtant, établir un pro-

fil type, n'implique-t-il par une uniformisation des recrutements ? L'usage de méthodes statistiques basées sur la classification et la fabrication de profils-type, n'est ainsi pas sans présenter un risque de clonage discriminatoire dans le recrutement.

Surtout, la fiabilité des prédictions de systèmes basés sur le *machine learning* dépend de la quantité de données collectées dans la base d'apprentissage. Cette incitation à collecter et accumuler met alors le fonctionnement même des IA en tension avec les problématiques du respect de la vie privée. Les tensions entre tenants du numérique et juristes autour des solutions fondées sur les big data RH (masse d'informations personnalisées sur les caractéristiques, les compétences et les performances des salariés) se cristallisent par exemple sur les questions de données personnelles. Or, la dimension éthique des outils de recrutement assistés par IA est un enjeu majeur, encore mal appréhendé (notamment en ce qui concerne le respect de la vie privée et les biais algorithmiques). Les exemples de promesses anti-discrimination, percutées par le fonctionnement intrinsèque des algorithmes, montrent ainsi la nécessité de résister à ce que Lacroux et Martin-Lacroux appellent une « illusion technologique »[61]. De même, dans le domaine de l'orientation, perçu comme un domaine éducatif où les individus sont encouragés, soutenus et guidés à réfléchir par eux-mêmes, il convient de remettre en perspective les modalités d'actions face à une numérisation qui atomise les individus, livrés à des algorithmes complexes. Le recours à l'IA doit ainsi, légalement s'accompagner d'une capacité à justifier et expliciter les décisions prises par des logiciels aux personnes qu'elles concernent. Alors que cette explicabilité des systèmes à base d'apprentissage constitue, en soi, un certain défi technique, elle se double également d'un impératif éthique pour ne pas voir favorisée une pseudo-efficacité au détriment de l'équité.

[1] Holland J. L. (1959), « A Theory of Vocational Choice », Journal of Counseling Psychology, 6(1): 35-45.

[2] Dumouilla A., Lamri J., « Chapitre 2. Évolution du rapport au travail et de l'orientation au xxe siècle », in Digitaliser l'orientation professionnelle. Les défis de l'accompagnement au xxie siècle, sous la direction de Dumouilla Auguste, Lamri Jérémy. Paris, Dunod, « Hors collection », 2022, pp. 43-60, [en ligne :] https://www.cairn.info/digitaliser-l-orientation-professionnelle--9782100827589-page-43.htm, consulté le 4 mai 2023.

[3] *Ibid.*

[4] Canzittu D., et Carosin E. (2020). « L'orientation scolaire et professionnelle face aux enjeux du 21e siècle : Rôle et fonction de l'école dans l'orientation tout au long de la vie ». In Psychologie de l'orientation tout au long de la vie, Dunod.

[5] Savickas M. L., Nota L., Rossier J., Dauwalder J.-P., Duarte M. E., Guichard J., Soresi S., Esbroeck R. V., Vianen A. E. M. Van, et Bigeon C. (2010), « Construire sa vie (Life designing) : Un paradigme pour l'orientation au 21e siècle », L'orientation scolaire et professionnelle, 39/1, pp. 5-39, [en ligne :] https://doi.org/10.4000/osp.2401, consulté le 4 mai 2023.

[6] Dumouilla A., Lamri J., « Chapitre 3. Sciences de l'orientation, vers un life design digital, éthique et durable ? », in Digitaliser l'orientation professionnelle. Les défis de l'accompagnement au xxie siècle, sous la direction de Dumouilla Auguste, Lamri Jérémy. Paris, Dunod, « Hors collection », 2022, pp. 61-97, [en ligne :] https://www.cairn.info/digitaliser-l-orientation-professionnelle--9782100827589-page-61.htm, consulté le 4 mai 2023.

[7] Cardoso, M., et Duarte, M. E. (2020). « Contribution à la recherche pour l'innovation dans le conseil en construction de carrière », in Psychologie de l'orientation tout au long de la vie, Dunod.

[8] Dumouilla A., Lamri J., « Chapitre 2. Évolution du rapport au travail et de l'orientation au xxe siècle », *op. cit.*

[9] Evans K. (2002). « Taking Control of their Lives ? Agency in Young Adult Transitions in England and the New Germany », Journal of Youth Studies, 5(3): 245-269.

[10] Dumouilla A., Lamri J., « Chapitre 3. Sciences de l'orientation, vers un life design digital, éthique et durable ? », *op. cit.*

[11] https://www.monkey-tie.com/raison-detre.

[12] Blons E., « Chapitre 6. La DRH : laboratoire et modèle du déploiement de l'IA », in L'entreprise disruptée. Les défis de l'IA pour les ressources humaines, sous la direction de Blons Emmanuelle, Paris, Dunod, « Hors collection », 2019, pp. 111-144, [en ligne :] https://www.cairn.info/l-entreprise-disruptee--9782100781461-page-111.htm, consulté le 4 mai 2023.

[13] Rico F., « Monkey Tie, le recrutement affinitaire ! », La France a d'incroyables start-up, octobre 2015, [en ligne :] https://wydden.com/startup-monkeytie, consulté le 6 avril 2023.

[14] Jakubowizc L.; « Pour son compte personnel d'activité, l'État a misé sur trois start-up de l'e-RH », Journal du Net, le 6 février 2017, [en ligne :] https://www.journaldunet.com/management/ressources-humaines/1191395-compte-personnel-d-activite-et-start-up-de-e-rh, consulté le 6 avril 2023.

[15] Diplômé d'Oxford et HEC Paris, il cumule 36 000 abonné sur son compte LinkedIn.

[16] Dumouilla A., Lamri J., Digitaliser l'orientation professionnelle. Les défis de l'accompagnement au XXIe siècle, Dunod, « Hors collection », 2022, ISBN : 9782100827589, [en ligne :] https://www.cairn.info/digitaliser-l-orientation-professionnelle--9782100827589.htm, consulté le 4 mai 2023.

[17] Il fait notamment partie des fondateurs du cercle d'entrepreneurs spécialisés dans le numérique Tomorrow Theory, https://tomorrowtheory.com/a-propos/#genesis.

[18] « Raison d'être », Site de l'entreprise, https://www.monkey-tie.com/raison-detre.

[19] Gray E., « Questions to Answer in the Age of Optimized Hiring », Time, le 11 juin 2015, [en ligne :] https://time.com/3917703/questions-to-answer-in-the-age-of-optimized-hiring, consulté le 4 mai 2023.

[20] Rampell C., « Your Next Job Application Could Involve a Video Game », The New York Times Magazine, le 22 Janvier 2014, [en ligne :] https://www.nytimes.com/2014/01/26/magazine/your-next-job-application-could-involve-a-video-game.html, consulté le 6 avril 2023.

[21] HireVue est une plateforme américaine de recrutement basée sur l'intelligence artificielle. Elle permet aux entreprises de mener des entretiens d'embauche à distance en utilisant des vidéos préenregistrées et des algorithmes d'analyse comportementale pour évaluer les candidats.

[22] Pyremetrics, aussi américaine, propose aux recruteurs les statistiques issues d'une douzaine de jeux cognitifs soumis aux candidats pour mieux les sélectionner.

[23] Blons E., *op. cit.*

[24] Cazals F., Cazals C., « Chapitre 5. Des machines et des maths », in Intelligence artificielle. L'intelligence amplifiée par la technologie, sous la direction de Cazals François et Chantal, Louvain-la-Neuve, De Boeck Supérieur, « Hors collection Économie/Gestion », 2020, pp. 75-93, [en ligne :] https://www.cairn.info/intelligence-artificielle--9782807331433-page-75.htm, consulté le 4 mai 2023.

[25] Corbille S., Foli O, et Tassel J., « Ce que les recruteurs font des outils numériques : pratiques, enjeux et paradoxes », Communication et organisation, 53|2018, 01 juin 2021, [en ligne :] https://doi-org.acces-distant.bu.univ-paris8.fr/10.4000/communicationorganisation.5955, consulté le 04 avril 2023.

[26] *Ibid.*

[27] *Ibid.*

[28] *Ibid.*

[29] *Ibid.*

[30] Corbille S., Foli O, et Tassel J., *op. cit.*

[31] L'architexte désigne des objets informatiques qui sont en position de régir l'écriture, de lui donner ses formats et ses ressources.

[32] Corbille S., Foli O. et Tassel J., *op. cit.*

[33] *Ibid.*

[34] Blons E., *op. cit.*

[35] *Ibid.*

[36] *Ibid.*

[37] *Ibid.*

[38] Blons E., *op. cit.*

[39] Lacroux A., Martin-Lacroux C., « L'Intelligence artificielle au service de la lutte contre les discriminations dans le recrutement : nouvelles promesses et nouveaux risques », Management & Avenir, 2021/2 (N° 122), p. 121-142. DOI : 10.3917/mav.122.0121, [en ligne :] https://www.cairn.info/revue-management-et-avenir-2021-2-page-121.htm, consulté le 4 mai 2023.

[40] Barocas S. et Selbst A.D. (2016), « Big data's disparate impact », California Law Review, n°104, p. 671, [en ligne :] https://ssrn.com/=2477899, consulté le 4 mai 2023.

[41] Garg N., Schiebinger L., Jurafsky D. et Zou J. (2018), « Word embeddings quantify 100 years of gender and ethnic stereotypes », Proceedings of the National Academy of Sciences, Vol. 115, n°16, pp. 3635-3644.

[42] Bolukbasi T., Chang K.W., Zou J.Y., Saligrama V. et Kalai A.T. (2016), « Man is to computer programmer as woman is to homemaker? Debiasing word embeddings », Advances in neural information processing systems, pp. 4349-4357.

[43] Lacroux A., Martin-Lacroux C., *op. cit.*

[44] *Ibid.*

[45] *Ibid.*

[46] *Ibid.*

[47] *Ibid.*

[48] *Ibid.*

[49] *Ibid.*

[50] Besse P. (2020), « Détecter et évaluer les risques des impacts discriminatoires des algorithmes d'IA », hal-02616963, 19.

[51] *Ibid.*

[52] Chabanet D., Cloarec M-A., Petani F. J. *et al.*, « L'appropriation intelligente de la transformation digitale : un processus collectif peu formalisé », Management & Avenir, 2021/2 (N° 122), pp. 171-192. DOI : 10.3917/mav.122.0171, [en ligne :] https://www.cairn.info/revue-management-et-avenir-2021-2-page-171.htm, consulté le 4 mai 2023.

[53] https://myskillcamp.com/fr/a-propos.

[54] Frouillou L., Pin C., Van Zanten A., « Le rôle des instruments dans la sélection des bacheliers dans l'enseignement supérieur. La nouvelle gouvernance des affectations par les algorithmes », Sociologie, 2019/2 (Vol. 10), p. 209-215. DOI : 10.3917/socio.102.0209, [en ligne :] https://www.cairn.info/revue-sociologie-2019-2-page-209.htm, consulté le 4 mai 2023.

[55] *Ibid.*

[56] *Ibid.*

[57] *Ibid.*

[58] *Ibid.*

[59] Cazals F., Cazals C., « Chapitre 13. L'IA est les allumeurs de réverbères », in Intelligence artificielle. L'intelligence amplifiée par la technologie, sous la direction de Cazals François et Chantal, Louvain-la-Neuve, De Boeck Supérieur, « Hors collection Économie/Gestion », 2020, pp. 257-280, [en ligne :] https://www.cairn.info/intelligence-artificielle--9782807331433-page-257.htm, consulté le 4 mai 2023.

[60] Radier V. « Les algorithmes sont une arme de domination sociale », L'Obs, 29 novembre 2018, [en ligne :] https://bibliobs.nouvelobs.com/idees/20181129.OBS6245/les-algorithmes-sont-une-arme-de-domination-sociale.html, consulté le 6 avril 2023.

[61] Lacroux A., Martin-Lacroux C., *op. cit.*

Benoît Debuigne est licencié en sciences géographiques (UCL) et détenteur d'un troisième cycle en aménagement du territoire et développement local (ULB). Aujourd'hui, il est animateur dans la thématique Lieux de vie & Espace public au sein de Citoyenneté & Participation.

Smart Cities

Obsolescence à programmer ?

Benoît Debuigne

Introduction

Depuis plus d'une quinzaine d'années, et ce partout sur la planète, nous assistons à l'émergence de « smart cities », autrement dit « villes intelligentes », « connectées » ou encore « 2.0 ». Pourquoi un tel enthousiasme vis-à-vis de la numérisation et de l'hyper-connectivité de nos territoires ? Dans un monde fortement urbanisé, les espaces urbains jouent un rôle prépondérant. En effet, aujourd'hui, 56% de la population mondiale vit en ville et 80% du PIB mondial y est produit [1]. Et, ce rapport de force a tendance à s'intensifier ces dernières années. Les villes doivent étancher leur soif de croissance, mais concurremment sont soumises à de nombreuses contraintes et défis. Selon Carlos Moreno (conseiller scientifique de Cofely Ineo[2]), nos cités doivent actuellement répondre à cinq enjeux majeurs : sociaux, culturels, économiques, écologiques et les résiliences. La forte pression démographique, des problèmes de congestion, de pollution, de pauvreté, de crise alimentaire… ne sont malheureusement que quelques exemples de défis auxquels les villes se trouvent confrontées quotidiennement et structurellement. Elles demeurent souvent le lieu d'expression de processus exacerbés les rendant extrêmement complexes à apprivoiser. Dans un tel contexte, l'optimalisation des services, des ressources et des usages des villes par la digitalisation semble être une piste alléchante.

Héritage de l'explosion technonumérique des années nonante et de la croissance urbaine, les smart cities ont bénéficié d'un terreau favorable pour s'implémenter. Si dix-neuf années se sont déjà écoulées depuis le défi de décongestion des centres urbains lancé par Bill Clinton au géant du numérique Cisco, la « ville du futur » ne relève plus totalement de la science-fiction. Dans la littérature, on cite couramment comme exemple les villes de Singapour, Séoul et Barcelone.

Preuve de cet engouement chez nous, en 2015, a été créé le Smart City Institute ; véritable centre de recherches universitaires dédié aux territoires durables et intelligents. Cet institut a pour rôle de référent académique Smart Region de la Région wallonne au travers de son programme Digital Wallonia. Ses missions se déclinent autour de quatre grands axes : la recherche, la formation, la sensibilisation et l'accompagnement des territoires wallons. La Région de Bruxelles-Capitale encourage également cette implémentation avec son projet de « Brussels Smart City » en collaboration avec le CIRB[3]. Les villes intelligentes s'inscrivent clairement dans l'approche numérique de nos Régions comme en témoignent les nombreux nouveaux appels à projets, et structures d'accompagnement… On peut citer quelques exemples comme l'appel à projets « Territoires intelligents » en Région wallonne, ayant notamment pour objectif d'encourager les villes et communes wallonnes à développer des projets numériques, en matière d'énergie, d'environnement, de mobilité ou encore de gouvernance. En Région bruxelloise, le projet « Fibru »[4], dont la commercialisation a commencé en 2024 mais ne couvre pas tout le territoire de la Région, traduisait une volonté d'accélérer le processus d'appui digital au territoire[5]. Concomitamment, l'Union européenne y fait référence dans son agenda urbain via notamment la Stratégie Europe 2020[6]. Elle vise une croissance durable, inclusive et intelligente grâce à une meilleure utilisation des technologies de l'information et de la communication (TIC) dans la gestion des services urbains, des infrastructures et de l'environnement citadin. Ceci démontre bien la place du numérique en matière de développement urbain visé pour les prochaines années. Chacune des échelles territoriales pourra (ou pas) s'approprier cette nouvelle manière de « construire et de vivre » la ville.

En quoi une ville peut-elle être intelligente ?

Mais, la question principale n'est-elle pas simplement : comment garantir une qualité de vie à l'ensemble des citoyens dans ces espaces en développement et en densification ? Les smart cities pourraient apporter des pistes de solutions à cette vaste interrogation. Néanmoins, est-ce la bonne voie à emprunter ? Souhaite-t-on vivre dans des villes administrées par des codes binaires, des algorithmes, des objets connectés au service d'ambitions prométhéennes[7] ? Faut-il poursuivre cette quête de la numérisation de nos territoires, s'en inspirer ou s'en dessaisir ? L'utopie pourrait-elle se transformer en dystopie ? Sujet à controverse, les smart cities suscitent pas mal de questionnements idéologiques, écologiques, technologiques… Mais, comme trop souvent, on peut observer que le progrès se développe plus rapidement que la réflexion éthique. Au travers des villes connectées, c'est le progrès lui-même qui peut-être questionné …

Cette analyse aura pour objectif principal d'interroger ces nouveaux modèles de développement et de gestion de nos villes. Nous essayerons de répondre modestement quant au sens à donner à cette évolution. Ce texte n'est donc pas un état des lieux exhaustif des potentialités offertes par les smart cities, et encore moins une approche technique. Par contre,

la conjoncture est propice à la critique, au bilan d'un modèle de développement urbain qui s'inscrit de plus en plus dans le paysage de nos villes. Dans un premier temps, un exercice sémantique sur le syntagme « smart city » sera proposé pour faciliter son appropriation. Ensuite, cette analyse s'attardera sur les principaux atouts et menaces du modèle de ville connectée. Finalement, une suggestion aux antipodes de la smart city sera proposée : la ville simplicitaire. Et nous terminerons par quelques recommandations afin que les villes s'inscrivent dans un développement soutenable et plus résilient.

1. Smart city, une genèse victime de sa précarité sémantique

Même si tout a commencé au début des années 2000 dans le quartier hyper connecté de Songdo en Corée du Sud, la paternité des villes intelligentes demeure difficile à attribuer. Nous verrons qu'il n'y a pas plus de consensus sur sa définition que *de facto* sur son opérationnalité. Sans trop nous attarder, le terme « smart », traduit généralement par « intelligent », pose lui-même une série d'interrogations. En quoi une ville peut-elle être intelligente ? Ce néologisme laisserait-il supposer que nos villes ou leurs concepteurs n'étaient pas assez éveillés ; et balayerait ainsi des siècles d'urbanisme et de politique de la ville ? Ou bien la ville dotée d'une forme d'intelligence serait-elle en capacité, cognitivement parlant, d'apprendre par elle-même, ce qui est le principe même de l'intelligence artificielle ? Le problème ne réside pas uniquement en sa définition généraliste et floue, mais aussi dans ses balises. À partir de quand peut-on s'autoproclamer smart city ? Effectivement, il n'est pas rare d'observer certaines villes ou certains territoires se décerner le titre de « smart » lorsqu'un espace est équipé d'une série de capteurs.

2. À titre d'exemple, voici deux définitions de smart cities

En 2015, l'Union Internationale des Télécommunications, agence des Nations Unies spécialisée dans les technologies de l'information et de la communication, a déterminé la Smart city comme « *une ville faisant usage des technologies de l'information et de la communication TIC, afin d'"améliorer la qualité de vie, l'efficacité de l'exploitation et des services urbains, et la compétitivité" tout en prenant en considération les "besoins des générations présentes et futures en ce qui concerne les aspects économiques, sociaux et environnementaux"* »[8]. Pour Michael Batty, architecte-urbaniste et géographe professeur à University College London, les smart cities sont « *des villes structurées par la genèse, la collecte, la gestion et le traitement instantanés et automatisés du big data*[9] *et des données urbaines produits en permanence par la technologisation des espaces et des réseaux urbains* »[10].

Comment est-on passé de la "ville durable" à la "ville intelligente" ?

Par ces définitions, on observe une différence notable dans leurs principales intentions. La première s'appuie davantage sur les finalités de la smart city comme catalyseur de la qualité du cadre de vie. Sous cette première définition, on y retrouve la grande majorité des villes intelligentes possédant une historicité et une vie déjà bien présente dans la cité. Le processus sera généralement transitoire et progressif. Citons comme exemple, Liège, Oslo ou encore Londres. La deuxième définition quant à elle mettra plus en évidence les moyens nécessaires et sa forme comme étant l'expression urbanistique de l'informatique ubiquitaire[11] et des objets connectés. Ce modèle de développement constituera généralement l'option de villes nouvelles avec une volonté de systématisation de la numérisation. Les exemples de Songdo en Corée du sud, de Xiongan en Chine ou de Masdar City à Abou Dabi en sont de parfaites illustrations.

Même s'il n'existe pas stricto sensu de label international définissant une ville comme étant smart, une multitude de classements sont diffusés chaque année récompensant « les bons élèves smart ». Un des index est produit par la Swiss business school Institute of Management Development et la Singapore University of Technology and Design (SUTD). Il est construit sur base d'indicateurs au sein de huit catégories : l'économie, la gouvernance, la technologie, la santé, la mobilité, l'environnement, la qualité de vie et la durabilité. En 2024, le top 5 était composé de : Zurich (Suisse), Oslo (Norvège), Canberra (Australie), Genève (Suisse) et Singapour (Singapour). Toujours selon ce classement, Bruxelles apparaît en 40e position sur 142 villes dans le monde devant des villes comme Barcelone, 81e ; San Francisco ; 75e ; Paris , 49e ; et Tokyo, 86e [12]. Avec toute la prudence liée à ce genre de classement, on peut souligner que ces dernières années notre capitale améliore la qualité globale de sa « *smartitude* »[13].

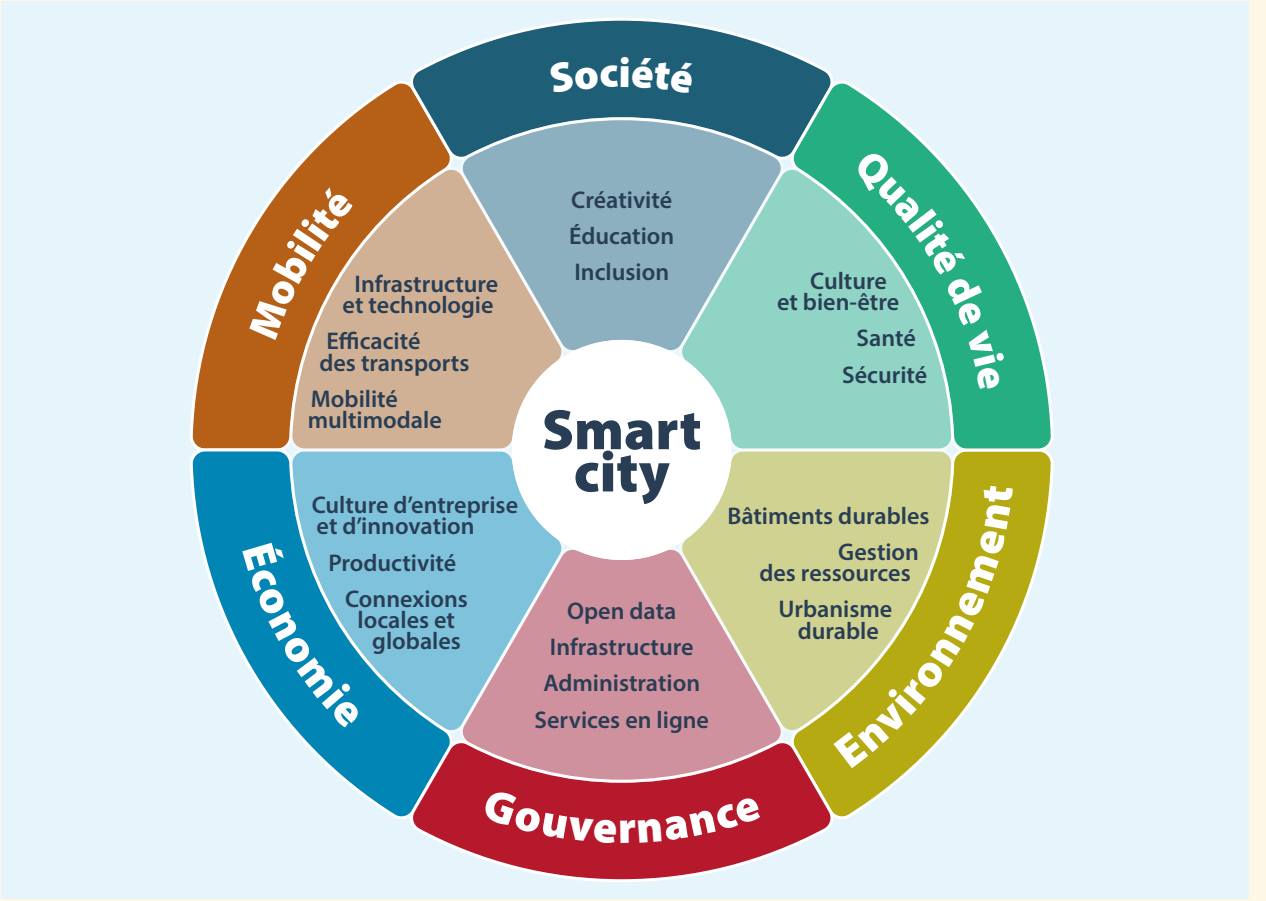
Prenons un peu de hauteur, et posons-nous la question de la place qu'occupent/occuperont nos villes intelligentes dans l'histoire de nos territoires ? Dernièrement, comment est-on passé de la « ville durable » à la « ville intelligente » dans la rhétorique urbaine ? On peut clairement s'interroger sur la continuité entre ces deux philosophies de développement de nos villes ! « *La ville durable voulait et veut sauver*

la planète… Cette ambition peu contestable dans sa formalisation a longtemps fait taire les critiques. Plus ambiguë dans ses objectifs, la ville intelligente a plus rapidement suscité les méfiances, entre suspicion de surveillance généralisée par les pouvoirs publics et mainmise des capitaux privés sur l'administration des villes »[14], mettant en lumière certaines limites des villes intelligentes et amorçant une partie de l'explication de la défiance, voire du scepticisme des citoyens sur lesquels nous reviendrons plus loin.

L'absence d'unanimité sur leur définition, paradoxalement, demeure propice à leur diffusion. Il est vrai qu'elles apparaissent comme un cristal aux mille facettes, complexe, protéiforme offrant de nombreuses opportunités pour répondre à des réalités et besoins extrêmement diversifiés. Elle s'inscrit dans des territoires et la spécificité de chacune d'entre elles se construit sur des besoins et des visions propres. La ville intelligente reste foncièrement une construction contextualisée trop peu mise en débat avec l'ensemble des acteurs. Le « piège » trop souvent observé lors de l'introduction de nouvelles technologies réside en l'exclusion sous prétexte de cette trop grande complexité et technicité. Tout comme la 5G, les projets smart sont régulièrement présentés comme des produits finis où les débats ne sont menés qu'à la marge.

3. Une pluralité des domaines au service de la métabolique urbaine

Dans quels domaines la smart city peut-elle s'exprimer ? Elle peut se traduire dans l'ensemble des dimensions de la « vie » d'une ville. Ci-joint un schéma reprenant les principaux items généralement rencontrés. Comme on peut le constater, les possibilités sont ex-



Source : https://be.brussels/fr/propos-de-la-region/la-strategie-brussels-smart-city.

trêmement variées, mais mettent fin aussi – pour le moment – à tout fantasme d'une ville smart à 100 % !

Dans une logique solutionniste et de services rendus aux usagers, les villes connectées, véritables tableaux polyptyque et holistique, semblent ainsi offrir des réponses aux grands enjeux des territoires. Malgré un discours universaliste, les dimensions smart ne sont pas l'apanage des villes riches des pays du Nord, en effet des villes comme Cotonou au Bénin ou encore Le Caire en Égypte s'en emparent aussi. Plus largement, on peut décliner le concept « smart » à toutes les échelles et tous les secteurs (smart ruralité, smart région, smart street…).

4. Vers une meilleure compréhension des villes ?

Les smart cities facilitent l'intelligibilité des usages de la ville, car être mieux informé, c'est être en capacité de mieux gérer. On peut donc dire que les données récoltées constituent un véritable atout d'aide à la décision pour les différents acteurs de la ville (politiques, administrations, partenaires et citoyens) … pour peu qu'ils y aient accès, puissent les exploiter, et en garder la maîtrise. Il s'agit aussi d'une réponse au déficit des connaissances de l'usage de la ville qui s'est d'ailleurs fortement complexifié ces dernières décennies. Hormis quelques études très coûteuses, les bases de données, indispensables à une bonne planification et gestion de nos villes, sont souvent trop simplistes notamment dans leur dimension temporelle. Thierry Paquot, professeur émérite à l'Institut d'urbanisme de Paris (université Paris-Est Créteil) souligne que la ville intelligente a introduit le temps à l'espace (chrono-aménagement) permettant une plus grande adaptabilité aux changements (résilience des territoires)[15]. En termes de qualité d'informations, la smart city équivaut à passer de la 2D à la 3D. Désormais, elle s'intéresse plus au métabolisme (son fonctionnement et son interactivité) qu'à sa morphologie (somme d'éléments qui la composent).

Autre atout intéressant pour les administrations, l'interconnectivité des données est un plus, mais passe également par une interconnectivité des services encore trop fréquemment cloisonnés. L'open data[16], par la libre circulation des données, faciliterait également le franchissement des frontières organisationnelles et/ou institutionnelles. Cette démocratisation de l'information rendrait visibles les flux, les consommations auprès de tous. Première étape vers l'adaptation et la résilience des villes et de leurs habitants.

5. Une matérialisation au service des citoyens ?

Nous allons parcourir quelques exemples concrets d'usages smart afin d'éclairer la potentialité que peuvent représenter ces villes connectées.

Le *smart water management* peut constituer un atout supplémentaire dans la lutte contre les inondations. Par exemple, la société Hydroscan située à Gembloux y travaille résolument. Leur algorithme combine les données de radars d'averses en temps réel, avec des cartes d'inondations pluviales déjà élaborées ? Hydroscan traduit ces données en prévision d'inondations en temps réel jusqu'au niveau de la rue[17]; une piste intéressante face à des évènements récurrents et fortement coûteux en vies et argent. Ce type d'outil « offrira » à la Région wallonne une meilleure compréhension de la gestion des risques et leur prévention.

Le car sharing permettrait de soustraire de l'espace public de cinq à dix voitures

Autre exemple, la fluidité de la mobilité reste une des préoccupations majeures des villes. La smart mobilité peut proposer des pistes de solutions à des problèmes complexes : congestion, pollution, baisse d'attractivité… Ainsi, la ville de Mons est équipée d'un projet « Smart Parking ». Celui-ci comprend notamment des capteurs sur chaque place de stationnement. Une application propose aux conducteurs d'être guidés vers une place libre, voire même de réserver celle-ci à l'avance. Cette solution permet une réduction des pertes de temps liées à la recherche d'un stationnement[18]. On pourrait imaginer des recherches plus fines via application : places pour personnes en situation de handicap, courte ou longue durée, véhicules lourds… Les possibilités sont évidemment très larges. Les systèmes de mutualisation au sein d'une ville connectée peuvent également être très bénéfiques en matière de mobilité. Selon Bruxelles Mobilité, le *car sharing*[19] permettrait de soustraire de l'espace public de cinq à dix voitures par voiture partagée[20].

Le projet « Smart led lighting » a permis à la ville de Wavre de réaliser 82 % d'économies via son éclairage public intelligent équipé de deux cent quatre-vingt-deux capteurs de présence. Ce système adapte l'éclairage public de façon dynamique ou « à la demande », c'est-à-dire uniquement en présence d'usagers sur la voirie, qu'il s'agisse d'un piéton, d'un vélo ou d'une voiture[21]. Les économies d'énergies et d'argent sont les principaux moteurs de ce genre d'installations. Les habitants sont généralement perturbés au début ; cette impression d'être suivi par la lumière, par quelque chose, par quelqu'un… Mais, une fois passées ces premières appréhensions, le sentiment de sécurité semble maintenu.

En matière de lutte contre l'inaccessibilité numérique, la ville de Tintigny a décidé de se doter de treize bornes wifi dans l'espace public offrant un réseau Internet gratuit à l'ensemble des citoyens. Ces installations pour un montant de trente-cinq mille euros ont été financées à hauteur de vingt mille euros par la commune[22]. La démarche se voulait aussi être un service aux touristes et gens de passage sur leur territoire aux nombreux atouts.

Le numérique peut-il doper la démocratie ?

Les services aux citoyens au sein de l'administration ne sont pas en reste non plus. À Bruxelles, l'e-administration via son IRISbox permet aux habitants de réaliser toute une série de démarches en ligne (extraits d'acte, changement d'adresse, certificats…). Il s'agit d'un gain de temps pour l'administration et pour les citoyens… pour peu qu'ils soient en possession d'une carte belge, d'un lecteur de carte et enfin d'un ordinateur… Ce qui est loin d'être le cas en particulier pour des publics plus précarisés ou plus âgés nécessitant toujours un accompagnement. La cohabitation de ces outils numériques avec les guichets traditionnels reste donc primordiale.

À Flobecq, des solutions innovantes ont été développées par Proximus grâce au soutien de la Région wallonne via l'appel à projets Digital Wallonia, lui-même financé dans le cadre du plan de relance. La ville s'est dotée de toute une série de technologies pour améliorer le quotidien des Flobecquois. Par exemple, l'éclairage Omniflow y augmente la sécurité des traversées de passages pour piétons via des capteurs, des caméras et de l'intelligence artificielle. On peut également compter sur des parkings sécurisés par des éclairages et des caméras de surveillance diminuant ainsi le sentiment d'insécurité. Des capteurs environnementaux ont aussi été déployés pour mesurer la qualité de l'air, et pouvoir agir rapidement en cas de besoin.

Au niveau touristique, la ville de Sanya en Chine a mis en place un système qui accompagne la gestion des lieux touristiques. Comment ? Une puce est insérée aux tickets d'entrée. Le système est conçu pour gérer le nombre de visiteurs sur les sites patrimoniaux, eux-mêmes contrôlés par un ensemble de capteurs (qualité de l'air, densité humaine, consommation électrique). Ici, la technologie se met au service qualitatif de l'expérience touristique…et de la surveillance.

Au sein des villes intelligentes, le numérique peut-il doper la démocratie ? Une approche plus centrée sur les habitants tend à considérer la smart city comme un lieu de renouvellement de la démocratie en réduisant la distance entre les citoyens et les politiques. Pour d'autres, la technologie rime avec entraves aux débats démocratiques comme pour Irénée Régnauld et Yaël Benayoun dans leur essai Technologie partout, démocratie nulle part (respectivement chercheur associé à l'Université Technologie de Compiègne et consultante – chercheuse indépendante en sociologie cofondateurs du Mouton numérique). Cet aspect a été développé dans ce cahier du numérique au travers de l'étude de notre collègue Philippe Courteille[23]. Autre point de vue intéressant, sur la smart gouvernance, Francis Pisani, dans son livre *Voyage dans les villes intelligentes entre datapolis et participolis*, pose le problème sous forme de tension entre deux pôles : *datapolis*, la ville entièrement gérée à partir des données recueillies par l'infrastructure technologique, et *participolis*, la cité dans laquelle les citoyens participent au design et à la gestion de l'espace dans lequel ils vivent. Si l'avènement du citoyen 2.0 n'est pas pour demain, aborder la question sous forme de « tension » peut sembler intéressant. Cette question de la smart gouvernance est tellement prégnante, mais aussi complexe, qu'elle mériterait une analyse en elle-même.

6. Smart cities, un scénario orwelien[24] en devenir ?

Les sentiments citoyens vis-à-vis des smart cities semblent contrastés oscillant entre enthousiasme et défiance voire méfiance. L'émergence de ces nouveaux modèles urbains techno- et data-centrés rend, par des équipements invisibles et des intentions peu transparentes, la ville intelligente paradoxalement inintelligible pour les citoyens.

C'est parfois même l'objectif et la vision politique qui sont remis en question. En effet, lorsque la finalité consiste plus en un outil géomarketing[25] et d'attractivité qui nourrit l'égoconception et/ou égoconstruction[26] de certains décideurs et technocrates, généralement les besoins des habitants ont peu de chance d'être rencontrés. Le danger serait de produire une ville disruptive sans réelle continuité urbanistique, sociale, environnementale…

De manière plus concrète, une smart city présente d'innombrables faiblesses à même de mettre parfois en péril la bonne gestion de la cité. En voici, quelques exemples.

7. Les smart cities, une opportunité pour les hackers

Les villes intelligentes s'exposent au piratage de leurs systèmes de gestion numérique. Certaines villes seront plus sujettes que d'autres face aux hackers de plus en plus nombreux. Une étude de 2020 de l'Université de Berkeley en Californie, appuyée par l'expertise de septante-six spécialistes en cybersécurité, défend que certains systèmes sont plus fragiles face à ces attaques. Dans leur rapport, les chercheurs rappellent que les systèmes d'urgence, de surveillance et certains types de signalisation routière, seraient les plus vulnérables. *A contrario*, les systèmes de gestion de l'eau seraient parmi les plus sûrs[27]. Malgré cela, en 2021, dans la ville de Oldsmar (Floride), une intrusion a eu lieu sur le système de gestion de l'eau permettant au pirate de changer temporairement les concentrations chimiques dans un système approvisionnement d'eau de ville[28]. Heureusement, sans trop de conséquences, car le piratage a été rapidement observé et les concentrations normales rétablies.

Autre exemple, le 1er septembre 2022, la société Yandex (équivalent de Google en Russie) s'est vu envoyer des dizaines de taxis à la même adresse à Moscou créant un embouteillage monstrueux. Si la situation a été relativement vite restaurée, elle démontre la fragilité et l'exposition des systèmes centralisés.

8. Des systèmes exposés aux pannes et dysfonctionnements

À cela s'ajoutent toutes les défaillances et pannes des différents réseaux. Sans rentrer dans une trop grande technicité, il est assez facile d'imaginer des situations bien plus dramatiques que celles-ci ! En plus des pannes d'électricité, une diffusion de données personnelles ou de paiement serait particulièrement à craindre. Pour exemple, en mai 2022, le groupe de hackers Lockbit a exigé une rançon auprès de l'intercommunale des soins de santé Vivalia (province du Luxembourg) suite à une cyberattaque au sein de six hôpitaux. La menace brandie demeurait en la diffusion d'informations personnelles de patients et de membres du personnel. Une évaluation des risques, des systèmes de protection et de leur réversibilité reste de ce fait fondamental. Quels sont les backups présents ? Quelle résilience les systèmes interconnectés offrent-ils en cas de dysfonctionnement ? Le coût de cette cybersécurité, généralement externalisée, se chiffre en millions d'euros pour des grandes villes… tout comme les conséquences d'une cyberattaque… Ces protections évoluent parallèlement au développement de nouvelles technologies, rendant obsolètes, ou inopérants, les outils sécuritaires d'une précédente génération. En cela, il est parfois impossible de mettre à jour des systèmes devenus fragiles, qui nous font dépendre de fabricants, de ressources limitées et dont l'obsolescence est encore trop souvent programmée.

9. Des cadres juridiques à la peine

Autre difficulté, les smart cities, synonymes d'innovation, représentent un véritable casse-tête juridique pour l'ensemble des acteurs (citoyens, administrations, politiques, sociétés privées…). En effet, les cadres légaux ne sont pas toujours adaptés à l'inclusion des nouvelles dimensions de ces villes. À l'heure où la juridiction sur la protection des données n'est pas encore consolidée, comment digérer cette dimension, incontestable soubassement des villes intelligentes ? L'ouverture et l'utilisation des données restent au cœur de la stratégie des grands groupes du numérique, qui exploitent ces « vides juridiques » afin de maximiser les profits via la réutilisation et la vente de données. Le règlement général sur la protection des données (RGPD), ou plus techniquement règlement UE 2016/679 du Parlement européen et du Conseil[29] définit les contours de la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il semble néanmoins insuffisant pour garantir l'anonymisation systématique des données et le « droit à l'intimité numérique ». De la même manière que nous protégeons notre intimité au cœur de nos foyers, nous devrions pouvoir également le faire au sein de la sphère numérique des bases de données des villes intelligentes. Ce choix doit rester possible, conscient et volontaire.

10. Un bilan carbone catastrophique ?

Quelle réelle empreinte environnementale pour ces villes parfois suréquipées ? Réponse difficilement appréciable. Et pourtant, la plupart des villes 2.0 et leurs opérateurs ignorent ou n'assument pas cette question arguant de solides bilans carbone. Cette question est pourtant cruciale dans le débat relatif à la pertinence du développement de ces villes. Il concerne aussi bien la production de leurs équipements, leurs usages, et leur recyclabilité. Quel est le rapport bilan carbone/coûts/bénéfices pour la ville ? Les impacts environnementaux, humains, géostratégiques… dépassent largement les frontières locales ! Pour illustrer ce propos, les villes intelligentes sont très gourmandes en capteurs, semi-conducteurs et autres composants. L'industrie des micropuces, actuellement toujours en crise, est l'une des plus consommatrices au monde en ressources et la souveraineté européenne en la matière est extrêmement faible. Clairement, ces productions sont décentralisées hors Europe, et plus particulièrement en Corée du Sud, à Taïwan et en Chine. À eux trois, ils représentaient, en 2022, 70 % de la production mondiale des semi-conducteurs[30].

Autre pierre d'achoppement, la question de l'empreinte carbone de l'ensemble de ces équipements et de leur fonctionnement reste trop peu objectivée mettant à mal les vertus des smart cities et la cohérence des discours sur leurs bénéfices environnementaux tant vantés par les villes et les opérateurs de services. Quasiment jamais, des chiffres qui mettent en balance le coût-bénéfice environnemental entre la production, la consommation et le démantèlement de l'ensemble des composants d'un projet smart ne semblent disponibles. L'exemple des éclairages LED pour l'espace public constitue une réelle économie d'énergie par rapport aux ampoules à décharge à haute densité, mais une fois connectés ces éclairages consomment de l'électricité en permanence, les capteurs ont un cycle de vie… Sans compter que le stockage et la circulation des données via notamment les data centers consomment de plus en plus d'énergie. « *La consommation des data centers croît de manière rapide avec l'arrivée de l'IA. Une requête auprès de ChatGPT consommerait ainsi 10 fois plus qu'une recherche Google et la consommation pourrait augmenter de 160 % d'ici 2030* », selon Goldman Sachs[31]. Comment un acteur public peut-il s'assurer de faire un choix environnemental au bilan carbone positif sans cette objectivation ?

Comment garantir pour les smart cities le "service après-vente" ?

Au-delà d'un bilan carbone en questionnement, comment garantir pour les smart cities le « service après-vente » et la continuité de production dans un marché mondial extrêmement tendu ? D'après la société Gartner[32], on comptait, en 2020, 9,4 milliards d'objets connectés[33] et 2,5 trillions d'octets de données générées chaque jour selon IBM[34]. Le coût énergétique, la pollution engendrée par les serveurs ou encore la fabrication de ces objets connectés sont gargantuesques. Faisons un exercice simple. En 2023, Charleroi totalisait 23 850 lampes publiques[35]. Si dans un projet de smart lighting, la ville ambitionnait de convertir l'entièreté de son réseau en gestion intelligente ce serait autant de capteurs, de détecteurs de présence nécessaires à son fonctionnement. Est-ce rentable ou bénéfique en tenant compte de l'ensemble du cycle de vie de ces équipements pour la ville, et plus globalement pour la planète ? La réponse est probablement non avec une efficacité aléatoire et une utilité réelle discutable. C'est sans compter sur les investissements pharaoniques requis pour des villes prises à la gorge financièrement. En revanche, opérer un choix éclairé (sans jeu de mots) en sélectionnant des « spots » prioritaires s'avérerait plus pertinent, plus en phase avec des objectifs environnementaux soutenus initialement.

11. Les villes intelligentes, terreau favorable à la surveillance numérique ?

Autre point noir au tableau ; la ville intelligente est perçue, et parfois utilisée, comme outil de surveillance panoptique[36]. Même si la ville intelligente peut être inclusive comme évoqué précédemment et sans tomber dans la caricature du totalitarisme numérique, elle peut se révéler très dangereuse dans ses dérives sécuritaires et autoritaires. On le sait, le risque est d'estomper la frontière entre les données personnelles et publiques. Concilier smart cities et vie privée restera un travail d'équilibriste. Selon Amnesty International, les villes intelligentes offrent un terreau propice à la surveillance numérique et discriminatoire. L'exemple de la persécution des Ouïghours en Chine est révélateur. Ce système de reconnaissance faciale est également capable de déterminer des « caractéristiques ethniques » et de les regrouper sous une étiquette, par exemple Han ou Ouïghour. Les informations recueillies par le système sont suffisantes pour déterminer où la personne est allée, quand et pour combien de temps, et permettent d'esquisser un tableau complet de la vie quotidienne de quelqu'un[37]. Plus récemment chez nous, l'utilisation de drones pendant la crise Covid-19 où la police pouvait constater les rassemblements et diffuser des consignes à respecter. Dans de nombreux domaines, l'histoire a démontré que technologisation rime régulièrement

avec déresponsabilisation. Même si ces technologies peuvent présenter des atouts intéressants, elles posent de nombreuses questions éthiques, juridiques… Rappelons que l'utilisation d'un drone par la police pour repérer une infraction dans un espace privé est interdite, et seul son usage dans un espace public est possible, mais conditionné notamment à la transparence de son utilisation. En effet, la loi sur la fonction de police du 5 août 1992 explique clairement les cas d'utilisation de caméras mobiles, drones compris. De plus, la circulaire ministérielle du 25 juin 2019 réglant l'usage de drones par les services de police et de secours définit quant à elle les exigences techniques pour les utiliser.

Cette absence de transparence sur le processus de « smartification » des territoires provoque des réactions urticantes dans certains cas, pour peu que les citoyens en aient écho. Bel exemple, la ville de Toronto en a fait les frais en 2017. Suite à un marché public, la ville a attribué à Sidewalk Labs (filiale de Google) la réhabilitation d'une friche portuaire urbaine pour en faire une vitrine publicitaire des nouvelles technologies. Cette société s'était engagée à financer l'entièreté du programme. Quelle aubaine pour une ville comme Toronto ! Le projet était passé de cinq à septante-sept hectares pour un budget de près de 1,3 milliard de dollars[38]. C'était sans compter sur un mouvement citoyen ! David contre Goliath. Les citoyens et associations ont gagné le bras de fer et le projet n'a finalement pas vu le jour. Quels étaient les arguments des associations ? Excès de caméras, de capteurs, opacité sur le respect de la vie privée et des données ainsi que leurs exploitations voire leur commercialisation. La ville de Toronto a essayé de sous-traiter via Waterfront[39] pour « rassurer » les habitants. Rien n'y a fait. La confiance était rompue. Quels enseignements peut-on tirer de cette expérience ? Tout d'abord, qu'il existe toujours des lieux de vigilance et de résistance citoyens efficaces. Ensuite, que les entreprises ne peuvent pas s'associer au secteur public aussi facilement sans en définir précisément les contours avec les citoyens, « clients finaux » de la ville connectée pour reprendre un terme utilisé par les opérateurs.

12. Vers une accélération de la privatisation des villes ?

Comme nous venons de le voir dans le cas de la ville de Toronto, n'oublions pas que les smart cities s'appuient, depuis leurs débuts, sur des démarches néolibérales 2.0 de groupes assoiffés par de nouveaux marchés. On y retrouve les grandes sociétés du monde numérique comme IBM, Huawai, Verizon, Cisco, Google… mais aussi des entreprises plus spécifiques comme Vinci, Urbanflow ou CITEOS. Par ces nouveaux partenariats publics/privés, nous assistons à une nouvelle forme de privatisation de la chose publique sous couvert d'accords de confidentialité imposés pour « protéger » des technologies innovantes (brevets technologiques). Ainsi, les grands gagnants seront ces acteurs privés alléguant détenir les solutions auprès des autorités locales souvent dépassées face à ces enjeux majeurs. Ce « solutionnisme » d'urgence ou l'approche thérapeutique d'une ville malade en devient le principal argument de collaboration. Ces sociétés se présentent comme le « messie » fournissant une solution « all inclusive » séduisante, ou dans une moindre mesure un service d'accompagnement. Dans un tel contexte et sans vigilance de la part de nos décideurs, nous assisterons/assistons à une privatisation progressive de nos services publics face à la place croissante du secteur privé dans la conception des stratégies urbaines. Nous passerions de la ville des élus à la ville des entreprises ; deux modèles ayant déjà démontré leurs limites. Prenons un cas extrême pour en illustrer les dérives possibles.

En Arabie saoudite, la ville de King Abdullah Economic City (KAEC) a pour objectif d'être un fleuron du « smart » avec près de deux millions d'habitants d'ici à 2035. Un partenariat public-privé a été conclu entre le gouvernement saoudien et un groupe immobilier de Dubaï, Emaar Properties. La ville n'a même plus de dirigeants politiques à sa tête. Elle est administrée par le président-directeur général d'Emaar Economic City (EEC), Fahd Al Rasheed[40]. Dans ce cas précis, le privé s'est substitué au politique.

En outre, ces mastodontes commerciaux arrivent avec des moyens considérables créant un rapport de force inversé par des contractualisations les protégeant, et extrêmement bien ficelées. Les marchés publics pour équiper nos villes sont de plus en plus complexes avec des sociétés juridiquement mieux armées pour garder la main. Autre difficulté rencontrée par les acteurs locaux, l'animation, la gestion et l'entretien se complexifient. Là aussi, les administrations n'auront pas toujours les moyens en personnels, en formations, financiers… pour assumer ces nouvelles fonctions. Fait parfois aggravant, la traçabilité de certaines sociétés ayant leur siège dans des paradis fiscaux ou leur volatilité pourrait également mettre en péril le suivi des projets (entretien et mises à jour des équipements et des systèmes). Les questions éthiques vis-à-vis de ces grands groupes sont donc particulièrement préoccupantes. Prenons le cas de la ville de Valenciennes. Elle s'est vu offrir gratuitement un système de surveillance par la société Huawai cultivant des liens étroits avec le gouvernement chinois. La ville devient non seulement un support publicitaire pour cette société, mais par ailleurs ces caméras ont aussi la possibilité technique de reconnaissance faciale telle qu'utilisée en Chine. Même si son usage est interdit en France et donc non opérante, la stratégie du pied-dans-la-porte est en marche[41].

13. Des équipements, entretiens, coûts de formations… souvent très onéreux

De manière générale, équiper une ville numériquement coûte très cher. Selon une étude menée par Mordor Intelligence[42], la taille du marché des villes intelligentes est estimée à 1,36 billion de dollars en 2024 et devrait atteindre 3,84 billions de dollars d'ici 2029, avec une croissance de 23,21% au cours de la période de prévision (2024-2029)[43]. À titre d'information, la Région wallonne investit 26,5 millions d'euros dans le cadre du Plan de Relance de la Wallonie (PRW) pour amplifier les actions liées à la connectivité sur son territoire. À cela s'ajoutent les subsides européens et les investissements des différents acteurs comme les intercommunales, les communes, le secteur privé…[44] Les smart cities ne seraient-elles que l'apanage des grandes cités dotées d'un effet de masse et de moyens financiers importants désertant ainsi les territoires plus petits et/ou moins bien nantis ? Pour ces derniers, leur numérisation passera probablement par la mutualisation de leurs investissements via des outils tels que les intercommunales. Mais il est évident qu'une sélection économique *per se* va naturellement s'opérer.

Hautement profitables théoriquement pour les citoyens, les projets smart peuvent aussi s'avérer à l'usage, être en dissonance avec l'objectif premièrement visé. Déjà en 2013, la ville de Nice s'était lancée dans un projet de smart mobilité qui lui avait coûté quinze millions d'euros. Échec cuisant, la ville a retiré l'entièreté de ses équipements (près de trois cents bornes intelligentes) et a remis ses anciens horodateurs. Le problème était l'inadéquation d'un système ayant pour objectif de limiter le temps de recherche d'une place en centre-ville. Comment l'expliquer ? Tout d'abord, le système n'était évidemment accessible qu'aux détenteurs d'un smartphone (discrimination par l'usage). Or le système a été financé par l'ensemble des citoyens y compris les personnes qui n'ont pas accès au numérique. Ensuite, le temps de disponibilité moyen d'une place libre en ville a été évalué à trente secondes rendant l'application inefficiente. Et enfin, comment faire respecter la loi sur les portables au volant quand il faut l'utiliser pour trouver une place ?[45] Comme on peut le constater avec cet exemple, une idée qui semble a priori bonne et louable (réduire la pollution en centre-ville) peut s'avérer relativement inadaptée, discriminatoire, dangereuse et coûteuse. Une solution contextualisée qui paraît de prime abord être une force peut devenir une faiblesse dans un climat innovant et parfois trop empirique.

14. Smart cities versus ville simplicitaire ?

Et si on prenait le contre-pied d'une ville hyperconnectée pour des espaces urbains où la sobriété numérique serait le maître mot. *Ceteris paribus* ces villes simplicitaires seraient-elles moins efficaces, moins agréables… ? En fin de compte, ne serait-ce pas le modèle qui apporterait la plus grande résilience face aux enjeux majeurs rencontrés ? C'est une vertu des idées simples que de vieillir moins mal que les autres. Mais, que peut recouvrir cette nouvelle vision de la ville ? L'Office de la langue française du Québec définit la simplicité volontaire, depuis 2002, comme un « *mode de vie consistant à réduire sa consommation de biens en vue de mener une vie davantage centrée sur des valeurs essentielles* »[46]. On pourrait tout à fait appliquer cette définition à la ville en concentrant les ressources et moyens. Il est indispensable de revenir à l'essence eutopique[47] même des villes, des territoires. Clairement, il s'agit là de l'antithèse des modèles de développement urbain actuels : les villes en transition ne sont plus suffisamment ambitieuses étant donné l'urgence des enjeux. Par ailleurs, dans un contexte de ressources limitées, le développement de villes intelligentes va probablement freiner/empêcher les désirs d'autres (concurrence territoriale). Par extrapolation de la phrase de Mahatma Gandhi[48], précurseur de la simplicité volontaire, on pourrait dire : « *Certaines villes devront se développer simplement pour que simplement d'autres puissent se développer* ». C'est aussi récupérer de la maîtrise pour les administrations et les citoyens en proposant des procédures plus lisibles, plus transparentes tout en limitant la technodépendance vis-à-vis du secteur privé.

De facto, leur matérialisation passerait par une simplification des procédures, des réseaux réduits à leur plus simple expression, des aménagements et éclairages publics présents, mais avec parcimonie… Grande naïveté diront les technophiles, indispensable diront les technophobes. L'approche ne doit pas forcément être aussi manichéenne. Dans toute chose, il y a lieu de pondérer et d'équilibrer la proposition. Pour exemple, peut-on envisager que les villes de New York ou Bruxelles déconstruisent certaines de leurs infrastructures ou équipements avouant des choix inopportuns et coûteux à leurs administrés ? Soyons raisonnables et voyons-le plus comme une opportunité de questionner de futurs équipements pour ne pas s'enfoncer un peu plus dans des cercles vicieux par des logiques d'investissements compensatoires (effet boule de neige).

Parallèlement, il y a lieu d'examiner une systématisation des nouveaux aménagements avec moins de complexité, moins de techno-dépendance et surtout moins d'empreinte environnementale. C'est ce qu'on appelle la techno-prudence. Fabienne Pasau (jour-

naliste pour la RTBF) évoque notamment le travail de Bernard Legros, instituteur et porte-parole du Mouvement des Objecteurs de Croissance, qui : « *décrit les technoprudents comme des gens qui réactualisent cette vertu qu'est la prudence : avant d'agir, on réfléchit, contrairement à ce que fait le libéralisme économique. Il utilise de préférence le mot "technoprudent", qui lui semble plus positif que le mot "technophobe"* »[49]. De nouveau, on peut tout à fait appliquer cette vision au développement de nos villes. L'utilisation parcimonieuse des technologies doit soutenir la sortie d'une logique dogmatique et de leur usage systématique, pour en faire l'exception au service des citoyens et de son environnement.

15. En conclusion, demain, comment composer avec les villes connectées ?

S'il est vrai que l'hypertechnologisation rend les systèmes de nos villes très exposés, trop coûteux, trop fragiles… et en partant du principe qu'une cohérence totale est impossible, faut-il conclure à leur mise au banc ? Au vu des éléments précédents, la réponse doit être nuancée. Une chose est claire, les villes vont devoir réaliser une forme de bilan de conscience vis-à-vis des choix stratégiques, écologiques, financiers… qu'elles vont opérer dans les années à venir.

Voici quelques points de vigilance pour que nos villes intelligentes puissent s'inscrire dans une vision de développement soutenable et résilient :

- La ville intelligente devra travailler l'association de l'inclusion sociale, des innovations technologiques et la réinvention urbaine, et ce au service d'une qualité de vie et un vivre-ensemble. Chaque nouveau projet « smart » se doit d'analyser les impacts sociaux et environnementaux de son implémentation pour en éviter des externalités négatives[50].
- Sortir de la logique selon laquelle une ville sans un projet de smart cities fort est une ville sans ambition. Elle ne doit en aucun cas constituer un nouveau dogme duquel elle ne pourra pas se défaire.
- Réaliser une étude préalable chiffrée et précise de l'impact environnemental, et ce sur l'entièreté d'un projet smart afin d'éclairer au mieux les décideurs, citoyens, acteurs quant aux coûts-bénéfices de leurs actions.
- Favoriser l'engagement ou la formation de fonctionnaires à ces nouvelles fonctions (citons les smarts manager, les data scientists[51]…) afin d'éviter d'externaliser ces services.
- Informer, vulgariser, former… les citoyens aux risques et opportunités de ces nouvelles technologies, ainsi que leurs impacts en leur donnant les moyens démocratiques pour le faire. Il est indispensable de soutenir toutes les approches collaboratives et de vulgarisation, que ce soit lors de la conception, de l'utilisation et de la gestion de ces outils numériques.
- Constituer des bases de données en open data, normalisées, anonymisées, évolutives, sécurisées et faciles d'utilisation.
- Mutualiser les projets et les investissements afin de procéder à des économies d'échelle. Développons l'intelligence de nos territoires par l'échange d'expériences.
- Renforcer la logique symbiotique entre durabilité et smart city. Dès lors, la ville intelligente doit se mettre au service de la durabilité de la ville, pour que la continuité surclasse la rupture. Selon le Smart city Institute de Liège, cette prolongation passera, dès le départ, par l'intégration et le suivi d'indicateurs environnementaux dans la stratégie des villes intelligentes, mais aussi en réfléchissant aux ressources mobilisées et favorables à l'équité et l'inclusion sociale[52]. La ville de Hambourg, connue mondialement pour son port, a limité la pollution atmosphérique en installant quelques dizaines de capteurs. Ces données en temps réel ont permis de fluidifier le trafic maritime et leur temps de chargement. Ici, clairement, les bénéfices rencontrés demeurent aussi bien environnementaux qu'économiques et sanitaires.
- Ne favoriser que les partenariats public-privé de qualité et sains où la maîtrise reste dans les mains de l'action publique.
- Anticiper la réversibilité des infrastructures, des équipements et du hardware[53] ou au minimum posséder des backups[54]. L'histoire de la géographie urbaine nous a démontré que le développement urbain est plus véloce que sa réversibilité en raison de son incroyable inertie !
- Encourager la propriété collective et la transparence des données, ainsi que leur utilisation préalable à toute démocratie.
- Réaliser des études exploratoires complètes de l'impact général d'un projet et proposer des lieux structurés de débats, de suivi et de contrôle pour accompagner les porteurs de projets et les citoyens.

Les villes vont devoir réaliser une forme de bilan de conscience

En définitive, la seule voie pour que nos territoires dits « intelligents » trouvent leur juste place est qu'ils soient élaborés dès le départ de façon à consolider un environnement de qualité, les droits élémentaires et les libertés pour tous les citoyens. Aussi longtemps que ces projets nourriront uniquement des opportunités économiques et sécuritaires, ils amplifieront le pouvoir de grands groupes technologiques et des gouvernements au détriment de l'environnement et des droits fondamentaux des habitants. Même si cette évolution semble inévitable en Occident,

le déploiement de villes intelligentes doit être maîtrisé. Dans un contexte d'étiolement des relations sociales, il est plus que temps de soutenir une ville des liens (*linking city*) où tous auront l'occasion de se rencontrer, de se parler, se fréquenter… pour une ville avant tout humaine, solidaire et soucieuse de son environnement. Si la ville intelligente peut y contribuer, alors elle survivra ! À chacun d'entre nous d'y être vigilant, et d'y contribuer !

[1] « Développement urbain : contexte », Banque Mondiale, [en ligne :] https://www.banquemondiale.org/fr/topic/urbandevelopment/overview, consulté le 3 octobre 2024.

[2] Filiale de GDF Suez Energie Services qui intervient sur des projets d'installations électriques industrielles et tertiaires, de réseaux d'énergie, d'éclairage public, d'infrastructures de transport et de télécommunications, de sécurité globale, de production d'énergie, de systèmes d'information et d'externalisation.

[3] Centre d'Informatique pour la région bruxelloise.

[4] Réseau public bruxellois de fibre optique et de gaines.

[5] Les opérateurs télécoms installent à toute vitesse des centaines de mètres de câbles sur les façades des maisons, créant une telle anarchie dans la Région bruxelloise que les bourgmestres se réservent d'intenter une action contre les opérateurs, Le Soir, Installation de la fibre : les bourgmestre bruxellois envisagent une action en justice, [en ligne :] https://www.lesoir.be/600901/article/2024-07-10/installation-de-la-fibre-les-bourgmestres-bruxellois-envisagent-une-action-en, consulté le 22 octobre 2024.

[6] « Communication de l'Europe 2020 : une stratégie pour une croissance intelligente, durable et inclusive », Commission européenne, [en ligne :] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52010DC2020&from=EN, consulté le 3 octobre 2024.

[7] En référence au mythe de Prométhée ; ambitions démesurées.

[8] Denolle A., La Smart city à l'heure du réchauffement climatique : un modèle fantasmé, Cairn, Droit et Ville, 2022/1 (N°93), [en ligne :] https://www.cairn.info/revue-droit-et-ville-2022-1-page-203.htm, consulté le 3 octobre 2024.

[9] Ensemble des données numériques produites par l'utilisation des nouvelles technologies à des fins personnelles ou professionnelles.

[10] Languillon R., « Derrière les mots : la smart city », La Fabrique de la cité, [en ligne :] https://www.lafabriquedelacite.com/publications/derriere-les-mots-la-smart-city, consulté le 3 octobre 2024.

[11] Tendance à intégrer des capacités de calcul via des microprocesseurs dans les objets de la vie quotidienne afin de les faire communiquer efficacement.

[12] « IMD Smart City Index 2024: Results In 2024 City Ranking Order and 2023 Ranking Comparison », International Institute for Management Development, [en ligne :] https://www.imd.org/smart-city-observatory/home, consulté le 3 octobre 2024.

[13] Contraction de smart et attitude.

[14] Offner J., « La smart city pour voir et concevoir autrement la ville contemporaine », Quaderni, 2018 [en ligne :] https://journals.openedition.org/quaderni/1172#quotation, consulté le 3 octobre 2024.

[15] *Ibid.*

[16] Données ouvertes dont l'usage et l'accès sont libres pour les usagers.

[17] « Un algorithme intelligent prédit les inondations urbaines jusqu'au niveau de la rue. Jusqu'à trois heures à l'avance », Hydroscan, [en ligne :] https://www.hydroscan.eu/fr/flood4cast, consulté le 3 octobre 2024.

[18] « La "Smart Mobility", une solution aux défis des villes d'aujourd'hui et de demain », La SPIE, [en ligne :] https://www.spie-ics.be/la-smart-mobility-une-solution-aux-defis-des-villes-daujourdhui-et-de-demain, consulté le 3 octobre 2024.

[19] « Aujourd'hui, on compte plus de 50 000 utilisateurs et d'utilisatrices réguliers (ndlr de carsharing) dans la capitale, un nombre qui a triplé depuis 2021. Les avantages sont nombreux : réduction du nombre de véhicules et donc d'émissions de CO_2, diminution des embouteillages, libération de l'espace en ville et baisse des coûts liés à la possession d'un véhicule », Environnement brussels, « Green deal Inclusive car sharing, l'auto partage plus utilisé, plus accessible et durable », 2024, [en ligne :] https://environnement.brussels/pro/nos-actions/projets-et-resultats/green-deal-inclusive-carsharing-lautopartage-plus-utilise-plus-accessible-et-plus-durable, consulté le 22 octobre 2024.

[20] « Les avantages d'autopartage », Bruxelles Mobilité, [en ligne :] https://mobilite-mobiliteit.brussels/fr/les-avantages-dautopartage, consulté le 3 octobre2024.

[21] « Eclairage Intelligent @ Wavre (Belgique) », Construction21, [en ligne :] https://www.construction21.org/belgique/infrastructure/h/eclairage-intelligent-wavre-belgique.html, consulté le 3 octobre 2024.

[22] « Tintigny : 13 bornes wifi ont été installées pour surfer gratuitement », L'Avenir, 28 septembre 2022, [en ligne :] https://www.lavenir.net/regions/luxembourg/2022/09/28/tintigny-13-bornes-wifi-ont-ete-installees-pour-surfer-gratuitement-KAR5MRWSP-RHSTCGA6O63NVHW3U, consulté le 3 octobre 2024.

[23] Courteille P., « Les dangers démocratiques du numérique », Citoyenneté & Participation, Étude n°48, novembre 2024, [en ligne :] https://www.cpcp.be/wp-content/uploads/2024/11/e48-danger-demo-numerique.pdf.

[24] En référence à l'univers post-apocalyptique de l'auteur George Orwell.

[25] Marketing d'un territoire prenant en compte sa dimension spatiale.

[26] Contractions d'égocentrique et de construction ainsi que conception.

[27] « The Cybersecurity Risks of Smart City Technologies : What Do The Experts Think ? », University of California Berkeley Center for long – term cybersecurity, mars 2021, [en ligne :] https://cltc.berkeley.edu/publication/smart-cities, consulté le 3 octobre 2024.

[28] « Dangerous stuff : hackers tried to poison water supply of Florida town », The New York Times, 8 février 2021, [en ligne :] https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html, consulté le 3 octobre 2024.

[29] « Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) », [en ligne :] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679, consulté le 3 octobre 2024.

[30] Gaudiaut T., « Technologie : quels pays peuvent fabriquer le plus de puces électroniques ? », Statista, [en ligne :] https://fr.statista.com/infographie/31385/capacite-mondiale-de-fabrication-de-semi-conducteurs-par-pays-region/#:~:text=Selon%20les%20donn%C3%A9es%20de%20l,%C3%A9levait%20%C3%A0%2013%20%25%20en%202022, consulté le 3 octobre 2024.

[31] Back E., « Un rapport révèle que les data centers consomment plus d'énergie qu'annoncé et menacent le monde d'une crise

électrique ! », Futura Sciences, 19 septembre 2024, [en ligne :] https://www.futura-sciences.com/tech/actualites/internet-rapport-revele-data-centers-consomment-plus-energie-quannonce-menacent-monde-crise-electrique-116101, consulté le 3 octobre 2024.

[32] Société américaine de conseil et la recherche en matière de technologie.

[33] Oksman A., « Pourquoi les objets connectés intéressent moins », Les Echos, 5 août 2020, [en ligne :] https://www.lesechos.fr/idees-debats/cercle/opinion-objets-connectes-comment-innover-a-lheure-de-la-sobriete-energetique-1228687, consulté le 3 octobre 2024.

[34] Guérin X., « Le temps réel, le véritable facteur de disruption des marchés », Les Echos, 30 mars 2018, [en ligne :] https://www.lesechos.fr/idees-debats/cercle/le-temps-reel-le-veritable-facteur-de-disruption-des-marches-132002, consulté le 3 octobre 2024.

[35] ORES Eclairage Public - Nombre de luminaires par commune (Annuel), ORES, https://www.odwb.be/explore/dataset/ores-eclairage-public-nombre-de-luminaires-par-commune-annuel/table/?disjunctive.arrondissement&q=charleroi&refine.commune=CHARLEROI, consulté le 3 octobre 2024.

[36] Dispositif spatial de surveillance en continu de la totalité d'un espace.

[37] Ekman A., « La Smart City chinoise : nouvelle sphère d'influence ? », Institut français des relations internationales, décembre 2019, [en ligne :] https://www.ifri.org/fr/etudes/la-smart-city-chinoise-nouvelle-sphere-dinfluence, consulté le 3 octobre 2024.

[38] « "Google City" de Toronto : les raisons d'un échec », Les Echos, 18 mai 2020, [en ligne :] https://www.lesechos.fr/idees-debats/cercle/opinion-google-city-de-toronto-les-raisons-dun-echec-1203831, consulté le 3 octobre 2024.

[39] Administration portuaire.

[40] Georges B., « KAEC, une ville à 100 milliard dans le désert saoudien », Les Echos, 7 janvier 2016 [en ligne :] https://www.lesechos.fr/2016/01/kaec-une-ville-a-100-milliards-dans-le-desert-saoudien-1109611, consulté le 3 octobre 2024.

[41] Faure A., « Smart cities : la stratégie de Huawei pour connecter nos villes de demain », Les Numériques, 2 janvier 2021, [en ligne :] https://www.lesnumeriques.com/vie-du-net/smart-cities-la-strategie-de-huawei-pour-connecter-nos-villes-de-demain-a157061.html, consulté le 3 octobre 2024.

[42] Société de consultance internationale en analyse des marchés située en Inde.

[43] « Analyse de la taille et de la part du marché des villes intelligentes – Tendances de croissance et prévisions (2024-2029) », Mordor Intelligence, [en ligne :] https://www.mordorintelligence.com/fr/industry-reports/smart-cities-market, consulté le 3 octobre 2024.

[44] « Digital Wallonia Giga Région. Nouveaux moyens au travers du Plan de Relance de la Wallonie », digitalwallonia.be, 19 juillet 2022, [en ligne :] https://www.digitalwallonia.be/fr/publications/prw-programme-giga-region, consulté le 3 octobre 2024.

[45] « Le stationnement dans la Smart City : les dérives du tout technologique ? », Candéliance, [en ligne :] https://www.candeliance.fr/stationnement-smart-city-derives-tout-technologique/#:~:text=La%20ville%20de%20Nice%20n,connect%C3%A9%20qui%20est%20en%20cause, consulté le 3 octobre 2024.

[46] « Définitions », Réseau québécois pour la simplicité volontaire, [en ligne :] http://www.simplicitevolontaire.org/la-simplicite-volontaire/definition, consulté le 3 octobre 2024.

[47] Lieu du bon, du bonheur.

[48] « Vivre simplement pour que simplement d'autres puissent vivre ».

[49] Pasau F., « La technoprudence : résister à la course effrénée du numérique », RTBF, 18 décembre 2017, [en ligne :] https://www.rtbf.be/article/la-technoprudence-resister-a-la-course-effrenee-du-numerique-10101167, consulté le 3 octobre 2024.

[50] Qui sont néfastes ou défavorables, qui causent une nuisance, un dommage.

[51] Ingénieur spécialisé dans le traitement des données.

[52] « Les villes peuvent-elles être à la fois intelligentes et durables ? », Smart City Institute, [en ligne :] https://www.smart-city.uliege.be/cms/c_7629106/fr/les-villes-peuvent-elles-etre-a-la-fois-intelligentes-et-durables, consulté le 3 octobre 2024.

[53] Élément qui désigne le matériel et les composants physiques qui composent les ordinateurs et leurs périphériques.

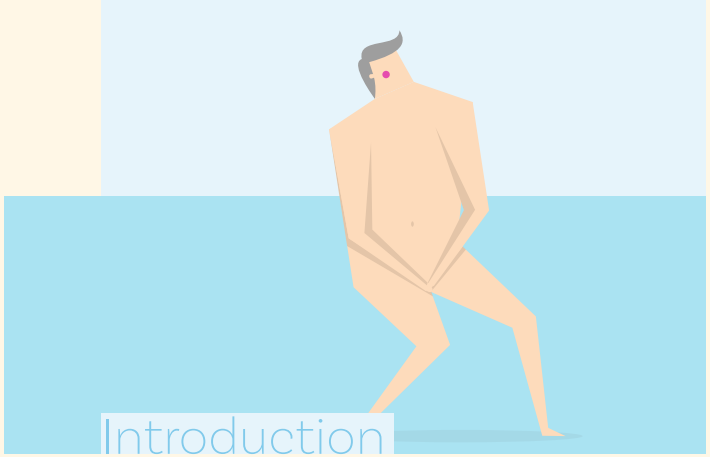
[54] Sauvegarde qui consiste à créer des copies de sécurité de sécurité et à les stocker.

Boris Fronteddu est chargé de recherche dans la thématique Consommation durable, au sein du pôle Recherche & Plaidoyer. Il est titulaire d'un master en journalisme ainsi que d'un master en politiques européennes.

Donner ses données

Une injonction permanente à la consommation

Boris Fronteddu



Introduction

Vous lisez probablement ces lignes depuis notre site web par le biais de votre ordinateur avec, peut-être, votre smartphone en poche et votre montre connectée autour du poignet. Et rien qu'avec cela, vous en dites déjà beaucoup plus que vous ne le pensez aux géants de la tech. Afin de pouvoir accéder à ce contenu, il vous a probablement été demandé d'accepter des « cookies ». Derrière ce nom évoquant un délicieux biscuit aux pépites de chocolat, se cache en réalité un *tracker* permettant aux pages web de mémoriser les traces que vous laisserez derrière vous suite à votre visite. Collectées en permanence, vos données personnelles sont ensuite compilées, traitées et croisées afin d'affiner sans cesse votre profil psychologique de consommateur. C'est cela qui en fait un bien valorisable. Et pour cause, deux cent trente « likes » sur le réseau social Facebook suffisent à un algorithme pour « *vous connaître mieux que votre propre conjoint* »[1]. Il convient désormais de rapporter cette information au nombre de traces que nous laissons quotidiennement sur le web pour se faire une idée de la quantité de données personnelles que nous fournissons aux géants du numérique. Chaque jour, nous générons, globalement, cinq cent millions de tweets, deux cent nonante-quatre milliards d'e-mails, quatre millions de gigaoctets de données Facebook, soixante-cinq milliards de messages WhatsApp et ajoutons 720 000 heures de nouveaux contenus sur YouTube[2].

Produire des quantités massives de données

Tout cela constitue donc une quantité astronomique de « données », soit d'informations sur notre vie personnelle, nos interactions sociales, nos centres d'intérêts, nos opinions politiques… Celles-ci représentent une manne considérable de revenus pour les entreprises numériques et particulièrement pour les géants de la Silicon Valley, les GAFAM (Google, Amazon, Facebook et Microsoft). Or, ce business model, sur lequel repose ces géants de la tech, a un coût. Écologique, puisque le stockage, toujours plus important, de ces données requiert sans cesse de nouvelles infrastructures très gourmandes en énergie, en eau et en espace. Démocratique, puisque la valorisation des données personnelles constitue une marchandisation de notre vie privée, de nos interactions sociales et, plus fondamentalement, de la vie humaine en elle-même. Politique, enfin, puisque ces données instaurent un contrôle permanent des citoyens, que celui-ci soit exercé par des entreprises privées, par les autorités publiques ou par les citoyens eux-mêmes.

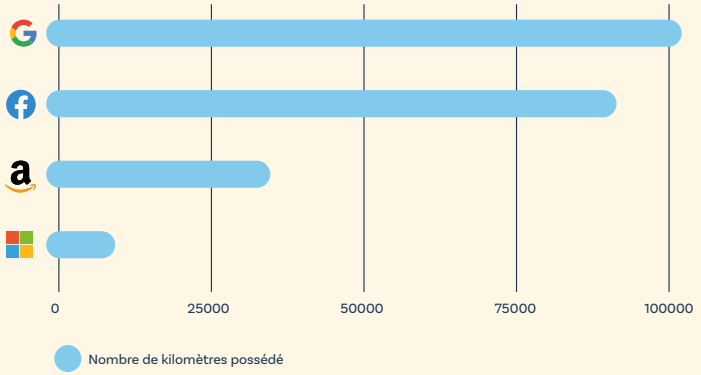
La première partie de cette analyse vise à définir ce qu'est la collecte, le stockage et le traitement des données personnelles. Elle permet de mettre en perspective les quantités de données collectées et la façon dont celles-ci se traduisent, matériellement. La deuxième partie, quant à elle, dresse un état des lieux du développement des data centers en Belgique et pose la question de la viabilité à long terme d'un tel modèle économique au regard de son impact environnemental. Dans le troisième chapitre, nous nous intéresserons aux limites auxquelles se sont heurtés d'autres pays européens face au développement inexorable des infrastructures de stockage et de traitement des données. La quatrième partie de cette analyse entend apporter une lecture plus politique à l'avènement de l'« économie des données » et à ce que celle-ci induit en termes de paradigme social et de déficit démocratique. Nous nous intéresserons, ensuite, aux raisons pour lesquelles ces données sont collectées et nous nous pencherons brièvement sur les relations incestueuses entre les géants de la tech, les services de renseignement et l'armée. Enfin, le dernier chapitre dressera un aperçu non exhaustif des outils législatifs existants pour encadrer les activités des GAFAM au sein de l'UE. Nous passerons en revue leur intérêt mais également leurs limites. La conclusion, pour sa part, apporte quelques éléments prospectifs dans le cadre d'une réflexion politique plus profonde.

1. Mise en perspective

Un article publié en 2018 sur le site web du Forum économique mondial affirmait que, contrairement au pétrole, pour qui la valeur dépend de sa rareté et de la difficulté grandissante pour l'extraire, il devenait « *de plus en plus facile de produire des quantités massives de données* »[3]. Or, cette appréciation des « données » en tant que « ressource » facile à produire et inépuisable tend à ignorer la matérialité de laquelle dépend leur génération et leur stockage. En effet, ceux-ci ne sont rendus possibles que par des milliers de kilomètres de câbles aériens, souterrains, sous-marins, des millions de serveurs, de relais et une quantité toujours plus importante d'énergie[4]. Et, aux infrastructures assurant le traitement, le stockage et le trafic des données, s'ajoutent les milliards de terminaux digitaux (ordinateurs, smartphones, objets connectés…). Comme l'illustre le graphique 1 ci-après, en 2024, Amazon, Google, Meta (Facebook, Instagram et WhatsApp) et Microsoft posséderont, à eux seuls, plus de deux cent mille kilomètres de câbles sous-marins. Parmi ceux-ci se trouve, notamment, le projet de

Meta qui vise à développer un câble sous-marin contournant l'ensemble du continent africain afin de relier les États du Golfe, l'Inde et le Pakistan connectant ainsi trois milliards de personnes. Ces infrastructures offrent aux GAFAM un contrôle considérable sur l'ensemble du flux de données qui transitent par ces câbles[5].

Graphique 1 :
kilomètres de câbles sous-marins appartenant aux GAFAM



En 2010, Google, Meta, Microsoft et Amazon possédaient un seul câble sous-marin longue distance. D'ici 2024, ce nombre sera supérieur à 30.

Source : BroadBandNow, via TeleGeography.

Concrètement, le stockage de données – peu importe la technologie utilisée – repose sur un découpage de l'information sous forme de codes binaires constitués de 0 et de 1. Un « octet »[6] désigne la plus petite unité de mesure pour quantifier l'information numérique et se compose d'une suite de huit chiffres (0 et 1), soit de huit « bits ». Dans ce cadre, la miniaturisation des appareils numériques signifie qu'ils deviennent de plus en plus complexes à concevoir puisqu'ils doivent permettre le stockage d'un nombre croissant d'informations par des pièces de plus en plus petites[7].

Dans ce cadre, les services en ligne pourraient être comparés à de gigantesques aspirateurs collectant en permanence les données des utilisateurs. La plupart des services en ligne, des réseaux sociaux à l'utilisation de moteurs de recherche en passant par l'utilisation d'une boîte mail, permettent à des sociétés privées de collecter les données de l'utilisateur. À cela s'ajoute la quantité toujours plus importante de données uploadées[8] d'une part, par les utilisateurs (notamment sur YouTube, sur le cloud…) et par les plateformes en ligne d'autres part (telles que Netflix, Amazon Prime, Spotify…). Les données générées par ces activités en ligne sont ensuite revendues à des publicitaires afin de cibler au mieux l'utilisateur. En d'autres termes, plus un utilisateur va consommer de services en ligne, plus il fournit des données qui permettront aux publicitaires de lui adresser des publicités « sur mesure » en ligne. L'utilisateur sera dès lors encouragé à consommer plus de biens et services en ligne, alimentant en retour l'accumulation de ses données personnelles et son « fichage » par les sociétés privées. Un « fichage » de plus en plus précis permettant en retour des publicités, elles aussi, de plus en plus adaptées[9]. En ce sens, la collecte et la valorisation des données sont directement liées à la société de consommation. Si l'on quantifiait l'impact environnemental et climatique du numérique en l'élargissant aux comportements de consommation liés à l'omniprésence de la publicité en ligne, celui-ci prendrait, en effet, des proportions encore bien plus importantes que les estimations généralement évoquées[10].

Les données générées sont revendues à des publicitaires

Pour appréhender la quantité de données stockées et en circulation, il convient de prendre un peu de hauteur. Un zettaoctet correspond à 8 000 000 000 000 000 000 000 000 bits. Pour comprendre ce que cela représente, imaginons qu'un bit corresponde à une pièce de un euro épaisse de trois millimètres. Un zettaoctet correspondrait à une pile de pièces de un euro longue de 2 550 années lumières, soit l'équivalent de six cents fois la distance entre la Terre et Alpha Centauri (le système solaire le plus proche). Or, en 2018, l'ensemble des données créées, collectées, copiées et consommées équivalait à trente-trois zettaoctets. Deux ans plus tard, en 2020, ce chiffre a presque doublé en passant à cinquante-neuf zettaoctets. En 2025, ces données devraient presque tripler et atteindre cent septante-cinq zettaoctets[11].

Dans la pratique, le stockage de données se réalise à plusieurs niveaux. Tout d'abord, des données sont stockées au sein même des appareils numériques personnels. Ensuite, certaines données sont stockées au sein d'institutions ou d'infrastructures locales tels que les serveurs internes des universités et des entreprises ou encore les tours de téléphonie mobile. Enfin, l'épicentre du stockage des données se situe au niveau des « data centers ». Il s'agit d'importantes infrastructures constituées de larges serveurs et occupées par un ou plusieurs opérateurs. Les serveurs doivent impérativement fonctionner en permanence, jour et nuit. En effet, une interruption signifierait une coupure dans le trafic de données au niveau local (par exemple, d'une entreprise) ou à un niveau plus large en fonction du type de data center (voir plus bas). Ainsi, une panne pourrait, par exemple, se traduire par la suspension des transactions bancaires, par l'impossibilité pour des entreprises d'assurer leurs tâches logistiques ou par l'incapacité pour des milliers d'utilisateurs d'accéder à leurs données professionnelles etc. Sans surprise, les entreprises gérant le plus grand nombre de data centers sont celles qui fournissent les principaux services de cloud, c'est-

à-dire des services de stockage de données en ligne pour les entreprises et les particuliers. Ce secteur est largement dominé par les géants du numérique et, notamment, les sociétés américaines Amazon, Microsoft et Google[12].

Parmi les data centers, certains sont particulièrement puissants ; il s'agit des data centers « hyperscale » comptant plus de cinq mille serveurs[13]. Ces infrastructures sont capables de stocker et de gérer des quantités colossales de données. Il existe environ six cents data centers « hyperscale » dans le monde, principalement localisés aux États-Unis et, dans une moindre mesure, en Chine, au Japon, au Royaume-Uni, en Allemagne et en Australie. Ces derniers sont, pour une grande partie, gérés par les géants du numérique. Amazon, Microsoft et Google gèrent, à eux seuls, plus de la moitié de ces data centers de grande envergure. Néanmoins, le plus grand data center au monde se situerait en Chine et serait géré par l'entreprise China Telecom Corporation Limited. Celui-ci s'étendrait sur plus d'un million de mètres carrés (soit l'équivalent de plus de nonante-deux terrains de football)[14]. L'entreprise dispose de cinquante-trois câbles sous-marins et de deux cent trente points de relais dans le monde[15].

Un data center pourrait engloutir deux cents litres de fioul par heure

Environ cent nouveaux data centers doivent être créés tous les deux ans pour assurer le stockage et l'échange de données au taux de croissance actuels. D'après Melvin Vopson, physicien à l'Université de Portsmouth au Royaume-Uni, si la production d'information digitale croît à un taux annuel de 50 %, d'ici un peu plus d'un siècle, la demande énergétique liée à celle-ci dépasserait la consommation énergétique actuelle de toute l'humanité. Un constat qu'il qualifie de « catastrophe de l'information »[16]. Les data centers sont, en effet, très gourmands en énergie[17]. Dans le détail, environ un tiers de le consommation énergétique de ces derniers est liée aux systèmes informatiques et les deux tiers restants sont liés au refroidissements, aux technologies de « back up » en cas de panne, à la sécurité et à la logistique[18]. En cas de panne, les data centers disposent généralement de batteries fonctionnant au fioul. Le cas échéant, un data center pourrait engloutir deux cents litres de fioul par heure[19].

Dans ce cadre, certains data centers entendent « verdir » leur consommation, cela suppose, par exemple, de remplacer ces groupes électrogènes au fioul par des batteries, par exemple, de type Lithium-Polymère (Li-Po). En effet, afin de faire baisser le bilan carbone des centres de données, il conviendrait d'être en mesure de stocker suffisamment d'énergie verte lors de pics de production pour pouvoir la rendre disponible lors de moments clés (par exemple, lorsque la météo ne permet pas de faire fonctionner les éoliennes). C'est par exemple, ce qu'a fait Google pour son data center situé à Saint-Ghislain en province du Hainaut. Il s'agit en effet du premier data center permettant le stockage d'électricité à grande échelle en vue de pallier l'intermittence des énergies renouvelables[20]. Néanmoins, généraliser un tel système à l'ensemble des data centers se heurterait, d'une part, à la disponibilité des matières premières nécessaires à la construction de ces batteries[21] et, d'autre part, aux impératifs de limitation de l'artificialisation des sols. Or, le changement climatique vient ajouter une pression supplémentaire à la situation déjà tendue de la disponibilité électrique pour les data centers. En effet, les températures ne baissent plus suffisamment l'été et l'humidité dans l'atmosphère tend à augmenter ce qui met à mal les systèmes de maintenance et de refroidissement des data centers[22]. Par ailleurs, certains data centers, comme c'est le cas pour Google à Saint-Ghislain, créent leur propre centrale de production énergétique. Le géant du numérique a, en effet, créé sa propre centrale solaire pour alimenter sa consommation. Néanmoins, si cette installation a permis à Google de communiquer sur le « verdissement » de ses activités, sa centrale solaire ne correspond, en réalité, qu'à un centième de la capacité électrique octroyée par Elia au géant de Silicon Valley[23] [24]. Autre spécificité du data center hyperscale de Google, à Saint-Ghislain l'utilisation de l'eau de surface, provenant d'un canal à proximité pour son système de refroidissement. D'autres data centers utilisent de l'eau potable ce qui, nous allons le voir plus bas, peut poser problème, notamment en période de sécheresse. Enfin, si les promoteurs de data centers insistent régulièrement sur les opportunités d'emplois que représente l'installation de telles infrastructures, il apparaît que celles-ci ne demandent en réalité que peu de main d'œuvre[25].

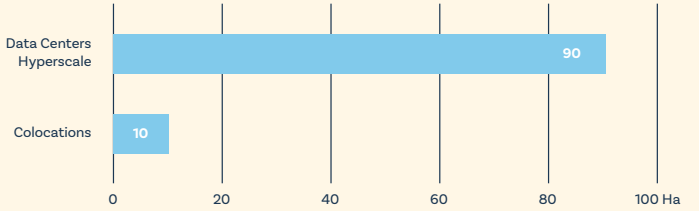
2. Les data centers en Belgique

Au total, l'ensemble des data centers situés en Belgique disposent d'une capacité de près de quatre cents mégawatts. Selon les estimations de la Belgian Digital Infrastructure Association, la Belgique compterait environ vingt-sept « colocation data centers ». Il s'agit de data centers détenus par des entreprises tierces louant leur capacité de stockage à des clients[26]. Ceux-ci disposent d'une capacité combinée de stockage et de traitement de l'ordre de quatre-vingt-cinq mégawatts. Or, seuls trois opérateurs gèrent cinquante de ces quatre-vingt-cinq mégawatts de capacité, en Belgique. Il s'agit de Proximus, LCL et Digital Realty. Par ailleurs, si la matérialité des données s'exprime en termes de serveurs et d'infrastructures, elle se traduit également par une occupation importante de l'espace. Au total, les colocation data centers occuperaient une surface de 100 500 m² en Belgique. Et cette surface est inéquitablement répartie entre Régions

puisque Bruxelles-Capitale concentre plus de la moitié de l'espace consacré aux colocation data centers. La Région bruxelloise est suivie par la Région flamande et, loin derrière, la Région wallonne qui ne représente que 7% de l'espace occupé par les colocation data centers.

Si la Région wallonne ne semble pas attirer les colocations data centers qui nécessitent une certaine proximité avec les entreprises clientes, elle dispose d'un profil particulièrement attrayant pour les infrastructures de plus grand envergure. Le seul data center « hyperscale » du pays est, en effet, situé à Saint-Ghislain, en province du Hainaut. Développé par le géant américain Google, il s'agit de l'un des plus grands data centers de ce type en Europe. Et pour cause, comme l'illustre le graphique ci-dessous, cette unique infrastructure occupe plus d'espace que l'ensemble des colocations data centers du pays et dispose, à elle seule, d'une capacité de nonante mégawatts. Le seul site de Google occupe neuf fois plus d'espace que l'ensemble des colocation data centers de Belgique[27]. Citée par la RTBF, la fédération d'entreprises Agoria Wallonie notait, par l'intermédiaire de sa directrice, que la Wallonie constituait une destination intéressante pour les grands data centers comparée à la Flandre qui est « beaucoup plus saturée que la Wallonie en termes de mètres carrés disponibles »[28].

Graphique 2
Surface au sol (en hectares) utilisée par les colocations et data centers hyperscale en Belgique, 2022



Source : Pb7 Research, 2022.

Les data centers hyperscale requièrent donc de larges espaces à prix « attractifs ». Et l'expansion rapide de ce secteur fait rapidement naître le besoin de nouvelles infrastructures. Ainsi, Google a d'ores et déjà annoncé de nouveaux plans d'extension cette fois à Charleroi et dans la région de La Louvière où elle a acquis un terrain trente-six hectares[29]. Le *data center hyperscale* de Google à Saint-Ghislain est, en effet, en constante expansion depuis le premier investissement de deux cent cinquante millions d'euros réalisé par l'entreprise américaine en 2007. Dès 2013, Google a investi trois cent millions supplémentaires pour accroître ses capacités de stockage et de traitement de données. Cinq ans plus tard et, à nouveau, en 2019, le géant du numérique a injecté, respectivement, deux cent cinquante millions et six cent millions d'euros pour étendre son data center. Dans le même temps, le site s'est doté d'une nouvelle centrale solaire pour son approvisionnement électrique. En 2021, l'entreprise annonçait un nouvel investissement de cinq cent millions d'euros pour agrandir le site. Au total, l'entreprise a donc investi trois milliards d'euros pour son data center de Saint-Ghislain[30]. Tout cela a eu pour conséquence de placer Google parmi les entreprises les plus consommatrices d'énergie de Belgique, aux côtés de géants industriels tels qu'Arcelor Mittal, le fabricant de produits phytochimiques BASF ou encore Infrabel, le gestionnaire de réseau de l'ensemble des lignes ferroviaires nationales[31].

Dans le même temps, Microsoft a annoncé la construction de trois data centers à proximité de Bruxelles. Ceux-ci auront, notamment, pour objectif de permettre aux entreprises qui disposent d'un compte Microsoft que celui-ci soit hébergé sur le territoire belge[32]. Et cette tendance va se poursuivre. La Belgian Digital Infrastructure Association estime que les nouveaux projets en cours devraient se traduire par le développement de 35 000 m² de nouvelles infrastructures en Belgique, soulignant que « *le marché belge [des data centers] devrait plus que doubler au cours des cinq prochaines années* »[33]. En l'état, la consommation électrique des data centers en Belgique représente 0,4 % de la consommation électrique totale du pays. Si cela peut paraitre anecdotique, il convient de souligner que leur consommation est concentrée au sein de « clusters » tels que Bruxelles et, nous l'avons vu, Saint-Ghislain. Cela signifie que « *l'accès au réseau énergétique dans ces zones pourrait devenir un défi pour les data centers si le secteur continue à se développer rapidement* »[34].

3. Trop de données ?

Ailleurs en Europe, la multiplication des data centers a déjà causé de sérieux problèmes en termes de demande énergétique, de gestion foncière et de consommation de ressources. La Région Île-de-France, à titre d'exemple – qui comptait cent vingt-quatre data centers en 2021 – doit gérer un réseau proche de la saturation tant en termes de demande électrique qu'en termes d'espace disponible. Rien qu'au nord de Paris, une vingtaine de data centers occupent plus de 100 000 m² de terrain[35]. D'ici 2030, les data centers installés au sein du Grand Paris devraient, à eux seuls, consommer autant qu'une ville d'un million d'habitants et constituer près de 25 % de l'augmentation des besoins énergétiques de la Région[36].

En juillet 2019, aux Pays-Bas, les municipalités d'Amsterdam et Haarlemermeer ont activé un moratoire suspendant l'implantation de nouveaux data centers. Les autorités publiques ont voulu, par ce biais, reprendre le contrôle sur la gestion du foncier et la consommation énergétique. Un an plus tard, les deux communes vont de nouveau autoriser la création de data centers mais sous certaines conditions ; ceux-ci devront s'installer au sein des parcs

déjà existants et ne pas excéder un certain plafond de consommation énergétique à moins de créer leur propre poste de transformation électrique[37]. Par ailleurs, en août 2022, au nord des Pays-Bas, un journal local a dévoilé qu'un data center occupé par Microsoft a utilisé, sur un an, quatre-vingt-quatre millions de litres d'eau, soit bien plus que ce que l'entreprise américaine avait initialement annoncé. En fait, le système de refroidissement du data center nécessite de l'eau lorsque la température extérieure excède vingt-cinq degrés. Or, la hausse des températures et les sécheresses sont précisément les raisons qui ont mené les autorités hollandaises à imposer des restrictions concernant l'utilisation de l'eau potable au cours de l'été 2022. Une situation qui a poussé des groupes locaux à s'interroger sur le fait que ces restrictions s'appliquent aux citoyens et pas aux géants de la tech[38].

Outre-Manche, le scénario apparaît similaire. Et pour cause, en Irlande, Microsoft et Amazon ont dû revoir leurs plans d'investissement visant la création de trois data centers. Une décision qui intervient après l'implémentation d'un moratoire sur le développement de nouveaux centres de données dans la région de Dublin du fait, notamment, de contraintes en termes de capacité électrique[39]. Le régulateur public irlandais avait, en effet, mis en garde contre la multiplication de black out si de nouveaux data centers continuaient à s'implanter dans le pays et, en particulier, dans la région de la capitale[40]. En Angleterre, les autorités publiques ont annoncé qu'il pourrait être impossible de construire de nouveau logements dans certains quartiers du sud-est de Londres jusqu'en 2035. En cause : la capacité du réseau électrique est mise sous pression par le « corridor de la Silicon Valley » au sein duquel se concentrent les data centers de la région[41].

Enfin, la Norvège offre également un exemple éclairant des risques liés au développement des infrastructures digitales. Le 26 mars 2023, le quotidien *Financial Times* relatait qu'une entreprise d'armement fabricant des munitions s'était vue refuser sa demande d'expansion. L'entreprise se trouve à proximité d'un data center occupé par le réseau social chinois TikTok, ce qui limite fortement l'offre électrique disponible[42]. Ce conflit entre industrie et data centers pour la disponibilité énergétique n'a rien d'anodin. Ces « goulots d'étranglement » devraient se multiplier en Europe, poussant les décideurs politiques à se positionner sur les activités économiques qu'ils considèrent « critiques ». Et ces choix seront d'autant plus difficiles à arbitrer que certaines entreprises stratégiques ne peuvent fonctionner que si elles sont en capacité d'accéder à des structures de stockage de données. En outre, nous l'avons vu, certaines données capitales telles que les données bancaires et hospitalières sont stockées au sein de data centers et limiter, voire réduire l'expansion du secteur pourrait s'avérer extrêmement complexe.

4. La vie humaine "colonisée"

L'ouvrage intitulé *The Costs of Connection. How Data is Colonizing Human Life and Appropriating it for Capitalism*[43] rédigé par le sociologue Nick Couldry et le professeur de communication à l'University de New York, Ulises Mejias, a introduit la notion de « colonialisme des données ». Celle-ci formalise l'idée que la collecte permanente de nos données personnelles repose sur la même logique que celle a justifié l'expansion des empires coloniaux européens au cours des derniers siècles. Cette logique reposerait ainsi sur sur quatre traits caractéristiques fondamentaux. En voici un bref aperçu esquissé sur base d'un résumé[44] réalisé par Dieter Decraene, chercheur à la KU Leuven au sein du Citip[45] :

+ L'appropriation des ressources : si, dans le cadre de l'entreprise coloniale, on pense généralement à l'exploitation des ressources naturelles et des populations colonisées, la collecte des données introduit une nouvelle appropriation des ressources. Il s'agit de l'appropriation de la vie humaine elle-même et de l'ensemble de nos relations sociales. Ceux-ci deviennent désormais « marchandisables » et représentent un enjeu commercial pour les sociétés collectant les données, les diffuseurs et les annonceurs publicitaires.
+ La formation de nouveaux ordres sociaux : la colonisation s'est bâtie sur l'imposition de nouveaux ordres sociaux par la force, structurant l'organisation au sein du territoire colonisé. Dans le cas du « colonialisme des données », ce nouvel ordre social s'impose par le biais de la digitalisation du quotidien, l'intégration des outils numériques durant toutes les étapes de notre vie et la numérisation de nos rapports interpersonnels.
+ Une concentration extrême de la richesse : alors que l'entreprise coloniale a permis aux empires d'accaparer et d'accumuler les richesses, notamment, par le biais de l'exploitation des colonisés et de leurs ressources naturelles, la collecte de données a permis à quelques géants du secteur de s'ériger en tant que puissance incontournable du secteur numérique. Une position qui leur permet d'accaparer la majeure part des bénéfices réalisés par le stockage, le traitement et la vente de données. À titre d'exemple, Google centralise 81% de l'ensemble des recherches sur Internet et 94% des recherches effectuées depuis un smartphones ; Android et iOS (iPhone), pour leur part, représentent 99% des systèmes d'exploitation des smartphones ; Meta, via ses services Facebook, Instagram, Messenger et WhatsApp, totalise, pour sa part, 2,47 milliards d'utilisateurs quotidiens[46]. Des chiffres qui témoignent d'un véritable règne sans partage de quelques grands opérateurs privés.

+ La création d'idéologies pour justifier les pratiques d'appropriation : la colonisation a, notamment, été rendue possible par l'acceptation du narratif de la « mission civilisatrice ». Le modèle de développement basé sur l'appropriation des données s'appuie, pour sa part, sur l'injonction à la connexion permanente et la nécessité d'être joignable à tout moment par ses amis, sa famille, son employeur… Qui n'a jamais reçu des remarques du type « tu n'as pas vu mon message WhatsApp ? je t'ai laissé quatre vocaux… » ou « tu n'as pas vu l'invitation à la soirée ? Je t'ai envoyé une invitation sur Facebook ». Autre exemple éclairant, celui de l'obligation de scanner un QR code pour obtenir un simple menu au restaurant, témoignant d'une intégration de plus en plus profonde du digital dans nos comportements sociaux.

Les individus sont devenus des "dividuels" et les masses, des données

Une autre analyse intéressante pour appréhender l'avènement d'une organisation sociale basée sur l'accaparement et le traitement des données est sans doute celle des « sociétés de contrôle », un concept développé par le philosophe français Gilles Deleuze. Au cours des années 1970, Foucault avait défini ce qu'il appelait les « sociétés disciplinaires ». Selon ce concept, la société organise des lieux d'enfermement tels que la famille, l'école, l'usine, les maisons de repos. Ceux-ci permettent au pouvoir de contrôler et d'organiser les forces productives de la société, de les discipliner. Gilles Deleuze, pour sa part, note que, désormais, les lieux d'enfermement tels que les hôpitaux, l'école et l'usine sont en crise. Il voit dans cette dynamique la fin progressive des sociétés disciplinaires et leur remplacement par ce qu'il dénomme « les sociétés de contrôle ». Celles-ci ne sont pas basées sur l'enfermement des individus mais sur une apparente liberté qui n'existe que dans le cadre d'un contrôle permanent des individus. Ainsi comme l'écrit Deleuze : « *Le langage numérique du contrôle est fait de chiffres, qui marquent l'accès à l'information, ou le rejet. On ne se trouve plus devant le couple masse-individu. Les individus sont devenus des "dividuels", et les masses, des échantillons, des données, des marchés ou des "banques"* »[47]. En ce sens, les appareils numériques ont fait de milliards d'individus des « dividuels » producteurs de données, alimentant « *des centaines, voire des milliers d'algorithmes chaque jour* »[48].

Dans ce cadre, l'évaluation qu'imposent certains services numériques (noter son chauffeur Uber, son livreur Amazon, son vendeur en ligne…) constituent un mécanisme de contrôle permanent. Et ce contrôle ne s'applique pas uniquement au fournisseur de services mais également à l'utilisateur puisque les données de ce dernier seront collectées et valorisées (le trajet que vous avez fait en Uber, le nombre de fois que vous avez commandé à manger, les centres commerciaux que vous avez fréquentés…)[49]. Le centre commercial City 2 à Bruxelles dispose d'un logiciel intitulé « footfall analytics » et offre, à ce titre, un exemple éclairant de la façon dont l'économie des données impose un contrôle permanent des individus. Le logiciel détecte tous les appareils mobiles ayant leur fonction Wifi ou Bluetooth activée. Si ce logiciel ne permettrait pas d'identifier l'identité des personnes qui pénètrent dans l'enseigne, il collecte néanmoins une série de données relatives au comportement des visiteurs. Devant quelle vitrine vous êtes-vous arrêté ? Avez-vous mangé une gaufre en réalisant votre shopping ? Quel trajet avez-vous réalisé au sein du centre commercial ? Toutes ces données sont ensuite analysées et traitées, par exemple, afin de moduler les loyers des commerces et le prix des espaces publicitaires en fonction de la fréquentation[50].

5. Pour la pub, le renseignement et la guerre

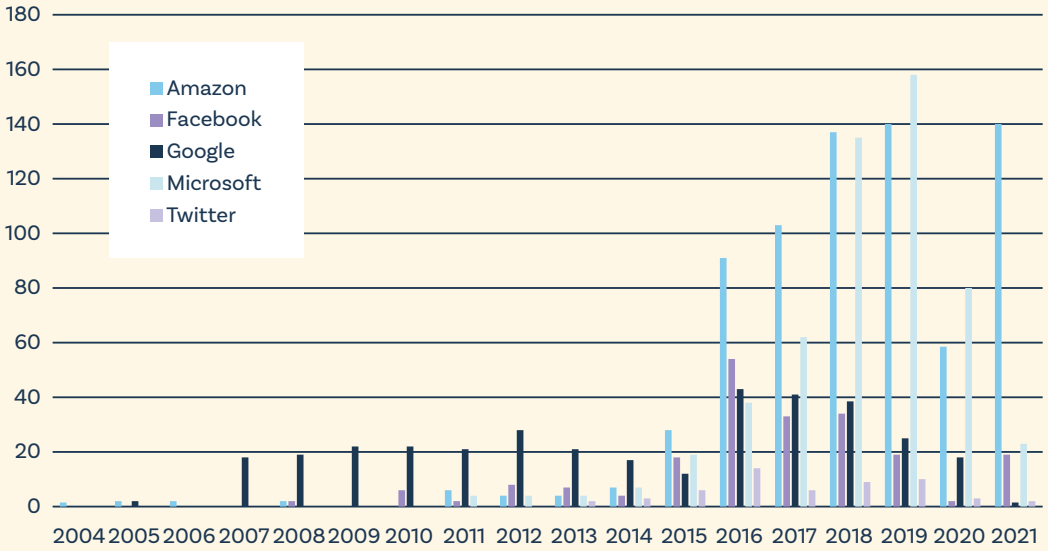
Nous l'avons vu, les géants du numérique, par le biais des données personnelles qu'ils collectent, jouent un rôle central dans la vente et l'achat d'espaces publicitaires en ligne. Ils offrent, en effet, aux annonceurs une fenêtre privilégiée pour atteindre directement les potentiels consommateurs en fonction de leurs intérêts, de leur lieu de vie, de leurs habitudes… Concrètement, au cours des microsecondes qui séparent le moment où un utilisateur clique sur une page web et le moment où celle-ci s'affiche sur son écran, des annonceurs publicitaires achètent automatiquement les espaces vendus à cet effet par la page web. Des algorithmes permettent ainsi à des annonceurs de viser le type de consommateurs qu'ils ciblent[51].

Ces transactions automatisées entre annonceurs et diffuseurs se font par le biais de « bourses » virtuelles au sein desquelles l'annonceur le plus offrant remporte l'espace publicitaire. Au sein de ce grand marché numérique, Google joue un rôle central. En effet, son outil de régie publicitaire sert d'interface, à la fois, aux vendeurs et aux acheteurs. Étant donné son poids sur le marché de la publicité en ligne – environ 90 % des parts de ce marché à l'échelle mondiale –, l'entreprise a été en mesure d'utiliser, durant des années, un système lui permettant de court-circuiter la concurrence. En utilisant les informations dont elle dispose du côté des annonceurs et des diffuseurs, l'entreprise a mis en place un système favorisant les acteurs utilisant son outil de régie publicitaire plutôt que ceux utilisant un outil concurrent[52]. Une pratique qui a permis à Google de générer des centaines de millions de dollars depuis 2013. Par ailleurs, afin de maintenir sa position dominante, Google a également réalisé un deal secret avec un

autre géant du numérique, Facebook, pour qui la publicité représente la part essentielle des revenus. Facebook a ainsi pu compter sur Google pour favoriser son propre régime de régie publicitaire[53]. Dans ce cadre, il apparaît que le ciblage publicitaire favorise la centralisation des données. En effet, cette centralisation permet de dresser des profils de consommateurs de plus en plus précis. Les services offerts par les géants de la tech servent donc à attirer l'utilisateur afin d' « aspirer » un maximum de données personnelles et à centraliser ces dernières dans le but de monétiser ces profils auprès d'annonceurs et diffuseurs[54].

Cela étant dit, si la relation entre la collecte de données, le ciblage publicitaire et la surconsommation peut être facilement établi, le « colonialisme des données » peut également servir à d'autres fins, notamment, militaires. Le recours à la collecte de données à des fins de surveillance de masse par le gouvernement américain avait d'ailleurs été mise en lumière en 2013 par les révélations de l'ancien employé de la CIA, Edward Snowden[55]. Dans le même temps, les GAFAM ont, eux-mêmes, développé des relations plus ou moins étroites avec le Département de la Défense états-unien. Comme l'illustre le graphique ci-dessous, en dix ans, les contrats passés entre les géants du numérique et les départements de sécurité US ont considérablement augmenté, en particulier, pour Microsoft et Amazon[56]. Il apparaît ironique, dans ce cadre, que le gouvernement américain se soit montré extrêmement critique à l'égard des relations que le réseau social TikTok entretient avec le gouvernement chinois[57].

Graphique 3
Les contrats de Big tech avec les Départements de sécurité US (2004-2021)



Source : Big Tech Sells War, 2022.

À la fin des années 1990, la CIA a créé un fonds, In-Q-Tel, destiné à investir dans les nouvelles technologies prometteuses, en particulier, au sein de la Silicon Valley. L'un des investissements les plus rentables d'In-Q-Tel se situait dans une entreprise dénommée Keyhole et dont l'activité visait à compiler des images satellites et aériennes afin de modéliser des cartes 3D. Cette technologie a d'ailleurs été utilisée par l'armée américaine dans le cadre de ses opérations en Irak au cours des années 2000. Dès 2004, Google a jeté son dévolu sur l'entreprise et a acheté Keyhole, alors rebaptisée Google Earth. Un deal qui « *a marqué le moment où Google a cessé d'être une société numérique tournée vers le consommateur et a commencé à s'intégrer au gouvernement américain* »[58]. Le fonds In-Q-Tel, pour sa part, continue de financer des entreprises actives dans le secteur du numérique. Parmi les projets qu'il finance, nous pouvons notamment citer Dataminr, un logiciel scrutant Twitter afin de déceler des menaces potentielles. En parallèle, le Pentagone collecte lui-même des quantités astronomiques de données par le biais de ses « avions espions »,

de capteurs, de caméras… Ainsi, la quantité de données est telle que le Pentagone se retrouve dans l'incapacité de traiter tout ce qui est collecté et cela « *même si l'ensemble de ses effectifs y consacraient leur tout leur temps* »[59]. Pourtant, le résultat de cette chasse aux données de données peut déjà s'avérer mortel. Au Pakistan, par exemple, les services de renseignement américains collectent des « métadonnées » issues de cinquante-cinq millions de téléphones portables. Des algorithmes traitent ces données et désignent ensuite les individus qui pourraient être impliqués dans des activités terroristes. Ces informations sont ensuite utilisées dans le processus de décision qui précède les frappes de drones[60]. Reste à répondre à cette épineuse question : quel est le poids de ces algorithmes dans le processus de décision ? Et, surtout, quelle est la marge d'erreur considérée comme tolérable par les autorités américaines ?

Quel est le poids de ces algorithmes dans le processus de décision ?

Cette utilisation des données à des fins de renseignement a également fait la une de l'actualité dans le cadre de l'emprise de la société chinoise Huawei sur le développement du réseau 5G au sein de l'UE. Les réseaux 5G de certains États membres dont celui de l'Allemagne et de l'Italie sont, en effet, largement dépendants de l'entreprise[61]. Une situation qui a notamment mené la Commission européenne à s'interroger sur les risques d'une telle exposition de l'infrastructure européenne aux ingérences étrangères[62]. De son côté, Pékin a déjà développé de puissants outils basés sur la collecte de données à des fins de renseignement et de contrôle. L'exemple le plus évocateur est sans doute celui du « crédit social », un score dont sont affublés les citoyens chinois sur base de données collectées sur les réseaux sociaux et par le biais de caméras intelligentes. Lancé en 2014, ce programme, déjà effectif dans quelques provinces du pays, a pour vocation de noter le comportement social des citoyens, par exemple, en fonction du nombre d'infractions routières qu'ils commettent. Un mauvais score peut se traduire par une série de sanctions telles que l'interdiction de prendre les transports en commun, d'acheter un bien immobilier ou de fonder une entreprise[63]. Du côté de l'Union européenne, le règlement européen sur les services numériques (DSA) devrait entrer en vigueur le 25 août 2023[64]. L'objectif de cette législation est d'encadrer plus strictement la publication de « contenus illicites » et de « désinformation » sur les plateformes en ligne, y compris, les GAFAM et d'autres très importants fournisseurs de services en lignes tels qu'Alibaba, TikTok ou encore Zalando[65]. Les fournisseurs de service concernés par la législation devront prévoir des mécanismes permettant aux utilisateurs de signaler rapidement les « contenus illicites ». En parallèle, les États membres devront se doter d'une structure spécifique dédiée à l'identification et au signalement de ces contenus. Leurs signalements feront l'objet d'un traitement prioritaire de la part des fournisseurs de service en ligne.

Le règlement prévoit également que les entreprises concernées fournissent certains algorithmes de leurs plateformes à la Commission européenne et aux États membres. En période de crise, comme par exemple la pandémie de Covid-19 ou l'invasion de l'Ukraine par la Russie, la Commission européenne pourrait prendre certaines « mesures d'urgence »[66]. À ce titre, le 10 juillet 2023 dans le cadre des émeutes qui avaient éclaté en France suite à la mise à mort du jeune Naël par un policier[67], le Commissaire au Marché intérieur, Thierry Breton déclarait au micro de BFM TV :

> « Lorsqu'il y aura des contenus haineux, des contenus qui appellent, par exemple, à la révolte, à tuer ou à brûler des voitures, [les plateformes] auront l'obligation dans l'instant de les effacer. Si elles ne le font pas, elles seront immédiatement sanctionnées. Si elles n'agissent pas immédiatement, on pourra non seulement leur donner une amende mais également interdire l'exploitation sur notre territoire [emphase ajoutée][68].

Si cette législation pourrait, en effet, se révéler utile pour lutter contre des phénomènes tels que la pédopornographie ou les appels à la haine raciale, elle pose également de sérieuses questions sur le contrôle exercé par les autorités publiques sur les actions militantes, syndicales, associatives… En particulier, en ce qui concerne la liberté de militer, de s'indigner et d'organiser des actions de désobéissance civile (comme le fait, par exemple, le collectif Extinction Rebellion[69] afin d'attirer l'attention sur les dégradations environnementales et le réchauffement climatique).

Tel que l'illustre ces exemples, le secteur des données est donc un instrument au service de l'industrie, puisqu'il permet un ciblage publicitaire permanent mais également un puissante arme au service du renseignement, de l'espionnage et de la guerre.

6. L'Union européenne protège-t-elle nos données ?

Le règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (communément appelé, règlement général sur la protection des données, « RGPD ») a été signé par le Parlement européen et le Conseil de l'UE le 27 avril 2016. Ce texte a constitué une petite révolution législative dans le monde numérique[70]. Dans le détail, le RGPD n'empêche pas la collecte de données personnelles. Le règlement a principalement pour objet d'encadrer le stockage de celles-ci. Il donne le droit à un utilisateur d'entamer des démarches pour accéder à ses données personnelles et, éventuellement, solliciter un effacement de celles-ci. Le règlement interdit également de transférer les données personnelles vers des juridictions qui ne disposent pas de la même législation. Depuis l'adoption du RGPD, environ cent septante pays ont pris des mesures des similaires. En ce sens, il s'agit d'une victoire politique pour l'UE.

Dans le quotidien des utilisateurs, la législation RGPD s'est principalement traduite par des bandeaux apparaissant à l'ouverture d'une page web lui demandant d'accepter ou de refuser les « cookies » et le traitement de ses données personnelles. Si l'utilisateur clique sur « accepter », ses données sont alors utilisées par des régies publicitaires (majoritairement détenues par Big tech, voir supra) à des fins de ciblage. Il n'est, par ailleurs, pas rare que certaines pages web conditionnent l'accès à leur contenu au fait d'accepter ce « traçage » en règle. Et, pour cause, les revenus publicitaires constituent parfois leur unique source de revenus. Or, le fait que le RGPD repose principalement sur la diligence de l'utilisateur (sommé d'accepter ou de refuser que ses données soient collectées et traitées) tend à déforcer la portée du texte. Citée par le magazine *Le Vif*, la Commission nationale de l'informatique et des libertés (la CNIL, l'autorité française des données) estime que « *60% des internautes français cliquent généralement sur "accepter" (…), la plupart des experts évoquant une "fatigue du consentement"* »[71].

Des experts évoquent "la fatigue du consentement"

Dans le même temps, l'interdiction du transfert de données vers des juridictions « plus laxistes » se révèle particulièrement complexe à mettre en œuvre. Et pour cause, en 2021, l'UE et les USA signaient un accord dénommé Privacy Shield qui devait encadrer le transfert de données d'une entité territoriale à l'autre. Or, les États-Unis disposent d'une législation permettant au gouvernement américain de solliciter directement des données personnelles auprès des entreprises américaines dont, les GAFAM. Rien qu'en 2021, le gouvernement américain aurait formulé près de cinq mille demandes auprès d'Apple et douze mille demandes auprès de Microsoft. Et ces demandes d'informations concernaient aussi bien des citoyens européens qu'américains. Dans ce cadre, la Cour de Justice de l'UE a invalidé l'accord signé entre les deux entités puisqu'il est impossible, pour les citoyens européens, d'accéder ou d'introduire un recours dans le cadre de cette utilisation de leurs données. Cela a mené trois États membres, l'Italie, la France et l'Autriche, à interdire Google Analytics, un logiciel de traçage des données personnelles qui se retrouvaient, *in fine*, envoyées aux États-Unis[72]. Face à la crainte de voir leurs services limités au sein de l'UE, Apple, Meta (regroupant Facebook, WhatsApp, Instagram) et Google se positionnent désormais en faveur d'une révision de la loi américaine[73].

Tel que l'illustre ce contentieux juridique, l'UE dispose d'une série d'instruments législatifs pour encadrer les activités de Big tech, notamment, le règlement européen sur les marchés du numérique, les règles européennes en matière de concurrence ou encore, nous l'avons vu, le RGPD. Ces instruments législatifs ont d'ailleurs permis aux autorités européennes d'infliger des amendes records au GAFAM. Parmi celles-ci, nous pouvons citer trois amendes pour un total de 8 milliards d'euros à Google dans le cadre de violations des lois antitrust, une amende de cinq cent soixante-et-un millions d'euros à Microsoft pour avoir imposé son propre navigateur internet ou encore des amendes, respectivement de quatre cent cinq millions d'euros relatif au traitement des données des mineurs et trois autres amendes pour un montant total de trois cent nonante millions d'euros pour non-respect du RGPD à Meta[74].

Bien que ces condamnations témoignent d'un cadre légal solide, ce dernier n'a pas fondamentalement affecté le business model des GAFAM. Et certaines associations dénoncent, pour leur part, un manque de diligence de la part de certains régulateurs. À titre d'exemple, le RGPD impose des « guichets uniques » pour les dépôts de plainte. Ceux-ci se situent dans le pays où l'entreprise concernée a installé son siège social européen. Pour d'évidentes raisons fiscales, c'est donc en Irlande que sont, notamment, installés Google, Facebook et Microsoft. Or, d'après l'ONG Irish Council For Civil Liberties, en 2018, le régulateur national irlandais a conclu des accords à l'amiable pour quarante-six plaintes sur un total de cinquante-quatre dossiers instruits. En outre, les sanctions appliquées se sont traduites par des amendes comparativement faibles. Une situation qui a mené le Comité européen de la protection des données à invalider 75% des sanctions formulées

par le régulateur irlandais et à solliciter l'imposition d'amendes plus élevées, notamment, pour la société Meta[75]. En outre, les moyens financiers des Big tech, leurs ressources juridiques couplées à d'intenses campagnes de lobbying[76] leur ont permis de s'adapter aux nouvelles exigences légales en comparaison à d'autres entreprises numériques qui ont dû réaliser d'importants investissements pour se mettre en conformité. Dans le même temps, le temps nécessaire à l'adoption de nouvelles mesures se heurte à la rapidité avec laquelle se développent de nouvelles technologies telles que l'intelligence artificielle.

Conclusion

À la lumière de cet article, il est permis d'affirmer que le modèle économique développé par les GAFAM est intenable. Alors que la quantité de données générées par l'activité en ligne est appelée à croître inexorablement, les infrastructures permettant leur stockage et leur traitement se heurtent d'ores et déjà aux limites énergétiques et naturelles des territoires qui les accueillent. Nous l'avons vu, en Norvège, les autorités publiques sont déjà contraintes de limiter le développement d'autres activités industrielles en raison de la quantité d'énergie consommée par un data center dédié au réseau social TikTok. Plus qu'un fait divers, cela signale l'avènement d'un véritable dilemme politique. En effet, l'industrie et, dans une moindre mesure, les autorités publiques se sont appuyées sur la numérisation pour gérer, contrôler et organiser l'ensemble de leurs activités. Se faisant, les géants de la tech ont réussi à se rendre indispensables au fonctionnement de l'économie et, plus largement, de la société, de son infrastructure jusqu'aux services publics les plus essentiels. Or, cette vulnérabilité à l'égard de Big tech complexifie fortement toute entreprise politique qui viserait à limiter son développement. À ce titre, il semblerait que les grandes entreprises numériques soient parvenues à « faire corps » avec les administrations publiques en leur fournissant toute une série d'instruments de contrôle et de renseignement. Le nombre de contrats passés entre les départements de sécurité US et les GAFAM démontre à quel point ceux-ci peuvent désormais constituer des acteurs à part entière de la gestion politique.

Plus fondamentalement, nous l'avons vu, l'« économie des données » repose sur le maintien et le développement de la société de consommation. Les données personnelles ne sont valorisables par les entreprises numériques que dans la mesure où elles permettent de cibler précisément les consommateurs. En ce sens, le *business model* des géants de la tech se révèle profondément incompatible avec un modèle de société évoluant dans le cadre des limites planétaires. Et pour cause, développer un quelconque modèle de société basé sur la sobriété apparaît impensable au sein d'une société dans laquelle règne en maître le ciblage publicitaire et l'injonction permanente à la consommation. Les différents moratoires à l'encontre de la construction de nouveaux data centers démontre néanmoins qu'il demeure possible – s'il existe une volonté politique – de freiner la fulgurante croissance de l'empire digital. Et cela, afin de repenser les priorités, notamment, en termes de consommation énergétique, de gestion d'espace et de préservation des ressources. De façon plus large, c'est la raison même de la « collecte » de données personnelles qui devrait être mise en débat. S'agit-il de collecter nos données pour faciliter notre prise en charge lors d'une hospitalisation ou pour nous proposer une livraison de fast food à l'heure précise où le sentiment de faim commence à nous parcourir ? Dans un cas comme dans l'autre, il est urgent de démocratiser cet enjeu en commençant avec une question fondamentale : est-ce bien utile et si oui, à qui ?

[1] « Après 230 likes sur Facebook, un algorithme vous connait mieux que votre conjoint », Lesinrocks.com, 13 avril 2018, [en ligne :] https://www.lesinrocks.com/actu/apres-230-likes-lalgorithme-de-facebook-vous-connait-mieux-que-votre-conjoint-139849-13-04-2018, consulté le 1er juin 2023.

[2] Volpson M., « The world's data explained – how much we're producing and where it is all stored », Theconversation.com, 4 mai 2021, [en ligne :] https://theconversation.com/the-worlds-data-explained-how-much-were-producing-and-where-its-all-stored-159964, consulté le 1er juin 2023.

[3] « You may have heard Data is the new oil. It's not », Weforum.org, 10 janvier 2018, [en ligne :] https://www.weforum.org/agenda/2018/01/data-is-not-the-new-oil, consulté le 20 avril 2023.

[4] Voir par exemple : « How does the internet cross the ocean ? », Weforum.org, 15 juin 2016, [en ligne :] https://www.weforum.org/agenda/2016/01/how-does-the-internet-cross-the-ocean/, consulté le 20 avril 2023.

« All internet servers together draw the world map », Stackscale.com, 21 mars 2022, [en ligne :] https://www.stackscale.com/blog/internet-servers-map/, consulté le 20 avril 2023.

[5] Jung M., « Digital capitalism is not a cloud. Exploring the extractivism at the root of the data economy », in Buxton N. (sous la direction de), State of Power 2023. Digital Power, Amsterdam : Transnational Institute, 2022, p. 67-77.

[6] Également appelé « byte ».

[7] Vopson M., *op. cit.*, 2021.

[8] Uploader signifie transférer des données vers un réseau informatique (par exemple, internet) à partir d'un terminal individuel.

[9] Borning A. *et al.*, « The 'Invisible' Materiality of Information Technology », Association of Computing Machinery, 2020, vol. LXIII, n°6, p. 57-64.

[10] Voir par exemple : Ferreboeuf *et al.*, « Environemental impacts of digital technology : 5-year trends and 5G governance », Shift Project.org, mars 2021, 47 p.

[11] Vopson M., « The world's data explained : how much we're producing and where it's all stored », Conversation.com, 4 mai 2021, [en ligne :] https://theconversation.com/the-worlds-data-explained-how-much-were-producing-and-where-its-all-stored-159964, consulté le 20 avril 2023.

[12] « Microsoft, Amazon and Google account for Over the Half of Today's 600 Hyperscale Data Centers », Srgresearch.com, 26 janvier 2021, [en ligne :] https://www.srgresearch.com/articles/microsoft-amazon-and-google-account-for-over-half-of-todays-600-hyperscale-data-centers, consulté le 20 avril 2023.

Bajpai P., « The Top Companies in the Cloud Computing Space », Nasdaq.com, 27 janvier 2023, [en ligne :] https://www.nasdaq.com/articles/the-top-companies-in-the-cloud-computing-space, consulté le 1er juin 2023.

[13] https://community.fs.com/blog/what-are-hyperscale-data-centers-and-how-do-they-work.html.

[14] Ce chiffre est à prendre avec précaution car les opérateurs tendent à cultiver une certaine opacité autour de la taille réelle de leurs data centers. Pour plus de nuances, voir : « Where is the world's largest data center ? », Greenenergydatacenters.com, 30 novembre 2022, [en ligne :] https://www.greenergydatacenters.com/eng/blog/where-is-the-worlds-largest-data-center, consulté le 1er juin 2023.

[15] Voir le site web de China Telecom : https://www.chinatelecomglobal.com/company/about-us.

[16] Vopson M., « The information catastrophe », AIP Advances, août 2020, vol. X, n°8, 085014, [en ligne :] https://pubs.aip.org/aip/adv/article/10/8/085014/990263/The-information-catastrophe, consulté le 20 avril 2023.

[17] Chavanne Y., « Inquiétude en Europe sur la consommation des data centrs », Ictjournal.ch, 21 septembre 2022, [en ligne :] https://www.ictjournal.ch/articles/2022-09-21/inquietude-en-europe-sur-la-consommation-des-datacenters, consulté le 1er juin 2023.

[18] Chiffres de 2013, voir : Debruyne O., « Saturé par les data centers, le réseau électrique d'Île-de-France va-t-il craquer ? », Leparisien.fr, 23 janvier 2023, [en ligne :] https://www.leparisien.fr/seine-saint-denis-93/sature-par-les-data-centers-le-reseau-electrique-d-ile-de-france-va-t-il-craquer-23-01-2020-8242308.php, consulté le 1er juin 2023.

[19] Marsac A., « Les data centers face à la flambée des prix de l'énergie "Aujourd'hui la seule solution neutre en carbone c'est le nucléaire" », Lalibre.be, 13 septembre 2022, [en ligne :] https://www.lalibre.be/economie/entreprises-startup/2022/09/13/les-data-centers-face-a-la-flambee-des-prix-de-lenergie-aujourdhui-la-seule-solution-neutre-en-carbone-cest-le-nucleaire-OOTWHWYMP5ALTAFRCDKBPCWF-DE, consulté le 1er juin 2023.

[20] « Une première mondiale à Saint-Ghislain : Google lance ses premières batteries de secours écologiques », Dhnet.be, 21 avril 2022, [en ligne :] https://www.dhnet.be/regions/mons/borinage/2022/04/21/une-premiere-mondiale-a-saint-ghislain-google-lance-ses-premieres-batteries-de-secours-ecologiques-MMYR5JYH5FA7XG3QFKAC52LTD4, consulté le 1er juin 2023.

[21] Voir Fronteddu B., « La matérialité de la "double transition". Jusqu'où vont-ils descendre ? », Bruxelles : CPCP, analyse n° 474, 2023, [en ligne :] http://www.cpcp.be/publications/materialite-double-transition.

[22] Marsac A., « Les data centers face à la flambée des prix de l'énergie : "Aujourd'hui, la seule solution 'neutre' en carbone, c'est le nucléaire" », Lalibre.be, 13 septembre 2022, [en ligne :] https://www.lalibre.be/economie/entreprises-startup/2022/09/13/les-data-centers-face-a-la-flambee-des-prix-de-lenergie-aujourdhui-la-seule-solution-neutre-en-carbone-cest-le-nucleaire-OOTWHWYMP5ALTAFRCDKBPCWF-DE, consulté le 24 avril 2023.

[23] Le gestionnaire du réseau de transport d'électricité à haute tension en Belgique.

[24] Quoidbach S. , « Les data centers menacent notre équilibre énergétique », Lecho.be, 23 novembre 2021, [en ligne :] https://www.lecho.be/opinions/edito/les-datacenters-menacent-notre-equilibre-energetique/10348416.html, consulté le 1er juin 2023.

[25] Tarczynska K., Money Lost to the Cloud. How Data Centers Benefit from State and Local Government Subsidies, Washington : Good Jobs First, 27 p, [en ligne :] https://www.goodjobsfirst.org/wp-content/uploads/docs/pdf/datacenters.pdf, consulté le 1er juin 2023.

[26] Ce chiffre exclut donc les data centers locaux c'est-à-dire internes à une société, une université, une institution publique…

[27] Vermeulen P., State of the Belgian Data Centers. 2022 Overview of the Belgian Data Center Market, Belgian Digital Infrastructure Association, octobre 2022, 45 p.

[28] Dath C., « Google investit à nouveau en Wallonie, qu'est ce qui attire le géant américain ? », Rtbf.be, 9 novembre 2021, [en ligne :] https://www.rtbf.be/article/google-investit-a-nouveau-en-wallonie-quest-ce-qui-attire-le-geant-americain-10875949, consulté le 1er juin 2023.

[29] Van Leemputten P., « Google achète un terrain à La Louvière pour la construction potentielle d'un nouveau centre de données », Levif.be, 24 octobre 2022, [en ligne :] https://datanews.levif.be/actualite/google-achete-un-terrain-a-la-louviere-pour-la-construction-potentielle-dun-nouveau-centre-de-donnees, consulté le 1er juin 2023.

[30] Voir : https://www.google.com/about/datacenters/locations/st-ghislain/, consulté le 1er juin 2023.

[31] Quoidbach S., *op. cit.*

[32] Martin A., « Les data centers de Microsoft s'installeront autour de Bruxelles », Lecho.be, 29 novembre 2022, [en ligne :] https://www.lecho.be/entreprises/technologie/les-datacenters-de-microsoft-s-installeront-autour-de-bruxelles/10431199.html, consulté le 1er juin 2023.

[33] Vermeulen P., State of the Belgian Data Centers. 2022 Overview of the Belgian Data Center Market, Belgian Digital Infrastructure Association, octobre 2022, 44 p., [en ligne :] https://bdia.be/en/insights/state-of-the-belgian-data-center-2022, consulté le 21 avril 2023.

[34] Vermeulen P., *op. cit.*, p. 33.

[35] Les impacts énergétiques et spatiaux des data centers sur les territoires, Paris : Institut Paris Région, Note rapide de l'Institut Paris Région, n°828, 2019, 5 p, [en ligne :] https://www.institutparisregion.fr/fileadmin/NewEtudes/000pack2/Etude_2171/NR_828_web.pdf, consulté le 24 avril 2023.

[36] Gonguet J.-P., « Peut-on gérer la croissance effrénée des data centers du Grand Paris ? », Latribune.fr, 8 mai 2015, [en ligne :] https://www.latribune.fr/economie/france/peut-on-gerer-la-croissance-effrenee-des-data-centers-du-grand-paris-474994.html, consulté le 24 avril 2023.

[37] Van Leemputten P., « Amsterdam autorise à nouveau les centres de données », Datanews.levif.be, 2 juillet 2020, [en ligne :] https://datanews.levif.be/actualite/amsterdam-autorise-a-nouveau-les-centres-de-donnees, consulté le 24 avril 2023.

[38] Vuijk B., « Datacenter Microsoft Wieringermeer slurpte vorig jaar 84 miljoen liter drinkwater », Noordhollandsdagblad.nl, 11 août 2022, [en ligne :] https://www.noordhollandsdagblad.nl/cnt/dmf20220810_68483787?utm_source=www.datacenterdynamics.com&utm_medium=referral&utm_content=, consulté le 1er juin 2023.

[39] Sundaravelu A., « Microsoft and Amazon scrap Irish data centre plans over power grid constraints », Metro.co.uk, 24 août 2022, [en ligne :] https://metro.co.uk/2022/08/24/microsoft-amazon-scrap-irish-data-centres-over-power-grid-constraints-17235104, consulté le 25 avril 2023.

[40] Tung L., « Massive data centre demands could lead to power blackouts, warns Ireland's utilities regulator », Zdnet.com, 14 juin 2021, [en ligne :] https://www.zdnet.com/article/massive-data-centre-demands-could-lead-to-power-blackouts-warns-irelands-utilities-regulator, consulté le 25 avril 2023.

[41] Corfield G., « The Energy Vampires sucking Britain's grid dry », Telegraph.co.uk, 1er août 2022, [en ligne :] https://www.telegraph.co.uk/technology/2022/08/01/energy-vampires-sucking-britains-grid-dry, consulté le 25 avril 2023.

[42] Milne R., « European ammunition maker says plant expansion hit by energy-guzzling Tik Tok site », Ft.com, 26 mars 2023, [en ligne :] https://www.ft.com/content/f85aa254-d453-4542-a50e-fa1171971ab0, consulté le 25 avil 2023.

[43] Couldry N. et Mejias U., The Costs of Connection. How Data is Colonizing Human Life and Appropriating it for Capitalism, Stanford : Stanford University Press, 2019, 352 p.

[44] Decraene D., « "Data colonialism" and the ubiquitous appropriation of human life », Law.kuleuven.be, 26 juillet 2022, [€n ligne :] https://www.law.kuleuven.be/citip/blog/data-colonialism-and-the-ubiquitous-appropriation-of-human-life, consulté le 1er juin 2023.

[45] Center for IT & IP Law, un centre de recherche de la Faculté de droit et de criminologie de la KU Leuven spécialisé dans les aspects juridiques et éthiques de l'innovation dans le domaine des technologies de l'information et de la propriété intellectuelle.

[46] Birch K., « There are no markets anymore. From neoliberalism to Big tech », in Buxton N. (sous la direction de), State of Power 2023. Digital Power, Amsterdam: Transnational Institute, 2022, p. 13-23.

[47] Deleuze G., « Les sociétés de contrôle », EcoRev', 2018, vol. XLVI, n°1, p. 5-12, [en ligne :] https://www.cairn.info/revue-ecorev-2018-1-page-5.htm, consulté le 1er juin 2023.

[48] Jung M., *op. cit.* ; pour aller plus loin, voir : Forest D., « Le « capitalisme de surveillance » et sa critique », Quaderni, 2022, n°105, p. 125-129, [en ligne :] https://journals.openedition.org/quaderni/2253, consulté le 13 juin 2023.

[49] Schwerer C.-A., « Comment l'économie numérique instaure une "société de contrôle" », Latribune.fr, 26 mai 2016, [en ligne :] https://www.latribune.fr/opinions/tribunes/comment-l-economie-numerique-instaure-une-societe-de-controle-572765.html, consulté le 1er juin 2023.

[50] De Rath R. et Sadutto M., « Vivons cachés : avec le "footfall analytics", souriez, vous êtes tracés ! », Rtbf.be, 31 janvier 2022, [en ligne :] https://www.rtbf.be/article/vivons-caches-avec-le-footfall-analytics-souriez-vous-etes-traces-10923790, consulté le 1er juin 2023.

[51] Birch K., *op. cit.*

[52] Bishop A., « Google's "Project Bernanke" Favors Google Over Other Advertisers », Searchenginejournal.com, 12 avril 2021, [en ligne :] https://www.searchenginejournal.com/googles-project-bernanke-favors-google-over-other-advertisers/402170/#close, consulté le 1er juin 2023.

[53] Tracy R. et Horwitz J., « Inside the Google-Facebook Ad Deal at the Heart of a Price-Fixing Lawsuit », Wsj.com, 29 décembre 2020, [en ligne :] https://www.wsj.com/amp/articles/inside-the-google-facebook-ad-deal-at-the-heart-of-a-price-fixing-lawsuit-11609254758?mod=article_inline, consulté le 1er juin 2023.

Horwitz J. et Hagey K., « Google's Secret "Project Bernanke" Revealed in Texas Antitrust Case », Wsj.com, 11 avril 2021, [en ligne :] https://www.wsj.com/amp/articles/googles-secret-project-bernanke-revealed-in-texas-antitrust-case-11618097760, consulté le 1er juin 2023.

[54] Hérard P., « Données personelles : peut-on lutter contre l'hégémonie des GAFAM ? », Information.tv5monde.com, 27 janvier 2018, [en

ligne :] https://information.tv5monde.com/international/donnees-personnelles-peut-lutter-contre-lhegemonie-des-gafam-28307, consulté le 1er juin 20230.

[55] Untersinger M., « Ce que les “révélations Snowden” ont changé depuis 2013, Lemonde.fr, 13 septembre 2019, [en ligne :] https://www.lemonde.fr/pixels/article/2019/09/13/ce-que-les-revelations-snowden-ont-change-depuis-2013_5509864_4408996.html, consulté le 1er juin 2023.

[56] Gonzalez R., « Militarising Big Tech. The rise of Silicon Valley’s digital defence industry », in Buxton N. (sous la direction de), State of Power 2023, Digital Power, Amsterdam : Transnational Institute, 2022, p. 35-47.

[57] « China criticizes possible US plan to force TikTok sale », Apnews.com, 23 mars 2023, [en ligne :] https://apnews.com/article/china-us-tiktok-security-technology-social-media-2245e433b5854010ebd99b7987fc78ca, consulté le 1er juin 2023.

[58] Yasha Levine cité dans Gonzalez R., *op. cit.*, p. 39.

[59] Gonzalez R., *op. cit.*, p. 40.

[60] Robbins M., « Has a rampaging AI algorithm really killed thousands in Pakistan? », Theguardian.com, 18 février 2016, [en ligne :] https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan, consulté le 1er juin 2023.

[61] Cerulus L., « Germany is (still) a Huawei hotspot in Europe », Politico.eu, 14 décembre 2022, [en ligne :] https://www.politico.eu/article/germany-is-still-a-huawei-hotspot-in-europe-5g-telecoms-network, consulté le 1er juin 2023.

[62] Déploiement des réseaux 5G au sein de l’UE : des retards et des questions de sécurité sans réponse, Luxembourg : Cour des Comptes de l’Union européenne, 2022, 73 p.

[63] Guedj L., « La Chine distribue des bons et des mauvais points à ses citoyens », Radiofrance.fr, 7 février 2019, [en ligne :] https://www.radiofrance.fr/franceinter/la-chine-distribue-des-bons-et-des-mauvais-points-a-ses-citoyens-9492388, consulté le 1er juin 2023.

[64] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), Bruxelles : Union européenne, JO L du 27 octobre 2022, p. 1-102, [en ligne :] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.FRA&toc=OJ%3AL%3A2022%3A277%3ATOC, consulté le 13 juillet 2023.

[65] Pour consulter la liste des grandes plateformes et moteurs de recherche concernés par le DSA : https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413, consulté le 13 juillet 2023.

[66] « Le règlement européen sur les services numériques (DSA) vise une responsabilisation des plateformes », Vie-publique.fr, 26 avril 2023, [en ligne :] https://www.vie-publique.fr/eclairage/285115-dsa-le-reglement-sur-les-services-numeriques-ou-digital-services-act, consulté le 13 juillet 2023.

[67] Séré L. et Leboucq F., « Nahel, conducteur de 17 ans abattu à Nanterre : les images qui mettent en cause le tir du policier », Liberation.fr, 27 juin 2023, [en ligne :] https://www.liberation.fr/societe/police-justice/hauts-de-seine-un-automobiliste-soupconne-dun-refus-dobtemperer-tue-par-la-police-20230627_HALNID55IFHZ7MXL6W7RCQCSDA, consulté le 13 juillet 2023.

[68] Mbembe L., « Couper les réseaux sociaux en cas de crise : une possibilité, pour Thierry Breton », Bfmtv.com, 10 juillet 2023, [en ligne :] https://www.bfmtv.com/tech/actualites/reseaux-sociaux/couper-les-reseaux-sociaux-en-cas-de-crise-une-possibilite-pour-thierry-breton_AV-202307100530.html, consulté le 13 juillet 2023.

[69] Voir : https://extinctionrebellion.fr.

[70] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Bruxelles : Parlement et Conseil de l’Union européenne, 27 avril 2016, JO L 119 du 4.5.2016, p. 1–88, [en ligne :] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

[71] « Malgré les amendes, le modèle des GAFAM perdure », Trends.levif.be, 22 mai 2023, [en ligne :] https://trends.levif.be/a-la-une/tech-medias/malgre-les-amendes-le-modele-des-gafam-perdure, consulté le 1er juin 2023.

[72] Romero J., « Google Analytics banned in several European countries due to GDPR violations », Chromeunboxed.com, 28 juin 2022, [en ligne :] https://chromeunboxed.com/google-analytics-banned-italy-europe, consulté le 1er juin 2023.

[73] Folon J., « On aura tout vu : Les GAFAM au secours du RGPD ! », Lesoir.be, 15 avril 2023, [en ligne :] https://www.lesoir.be/507318/article/2023-04-15/aura-tout-vu-les-gafam-au-secours-du-rgpd, consulté le 1er juin 2023.

[74] « La longue liste des contentieux de l’UE avec les Gafam et combien ont-ils rapporté », Trends.levif.be, 10 janvier 2023, [en ligne :] https://trends.levif.be/entreprises/la-longue-liste-des-contentieux-de-lue-avec-les-gafam-et-combien-ont-ils-rapporte, consulté le 1er juin 2023.

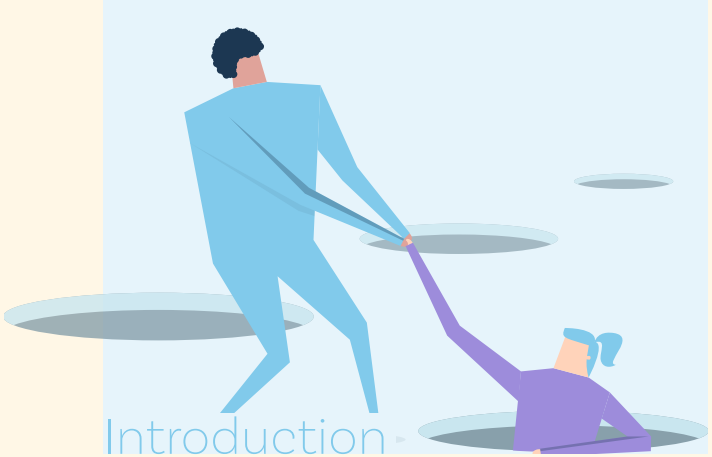
[75] Leloup D., « Cinq ans après le RGPD, des GAFAM ménagés par la CNIL irlandaise, Lemonde.fr, 14 mai 2023, [en ligne :] https://www.lemonde.fr/pixels/article/2023/05/14/vie-privee-cinq-ans-apres-le-rgpd-des-gafam-menages-par-la-cnil-irlandaise_6173359_4408996.html, consulté le 1er juin 2023.
Voir également : « Les GAFAM échappent au RGDP, la CNIL complice », Laquadrature.net, 25 mai 2021, [en ligne :] https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil, consulté le 1er juin 2023.

[76] Bouquet J., « Face à la puissance des lobbys des GAFAM, l’Union européennefait-elle le poids ? », Rtbf.be, 15 décembre 2020, [en ligne :] https://www.rtbf.be/article/face-a-la-puissance-des-lobbys-des-gafam-lunion-europeenne-faitelle-le-poids-10654184, consulté le 1er juin 2023.

Boris Fronteddu est chargé de recherche dans la thématique Consommation durable, au sein du pôle Recherche & Plaidoyer. Il est titulaire d'un master en journalisme ainsi que d'un master en politiques européennes.

La matérialité de la "double transition"

Jusqu'où vont-ils descendre ?



Introduction

Cette analyse se concentre sur l'amont de l'impact matériel de la digitalisation et de la transition énergétique, à savoir, l'extraction des matières premières nécessaires à la production des terminaux et infrastructures. Cette étape inéluctable pour l'existence même du secteur numérique connaît un regain d'intérêt de la part des décideurs politiques et, notamment, de la part de la Commission européenne. Et pour cause, le Pacte vert pour l'Europe – la stratégie à long terme de l'Union européenne qui vise la neutralité carbone à l'horizon 2050 – devrait s'appuyer sur une « double transition » ; énergétique et numérique[1]. Dans ce cadre, la Commission européenne a publié le 16 mars 2023, le *Critical Raw Material Act* (composé d'une proposition de règlement et d'une communication)[2]. Celui-ci appelle à relancer l'industrie minière au sein de l'Union européenne ainsi qu'à mettre la main sur de nouvelles sources d'approvisionnement en matières premières critiques. Cette proposition législative répond à un constat : la demande en métaux dans le cadre de la double transition est appelée à exploser et l'Europe ne produit qu'une part infime des métaux nécessaires à la double transition. En outre, l'offre de certains métaux critiques pour la transition énergétique et la digitalisation pourrait ne pas suffire pour répondre à une augmentation si conséquente et rapide de la demande.

L'idée d'une « immatérialité » du numérique entretenue notamment par des concepts tels que le *cloud* (sorte de « nuage » où seraient stockées les données) et les plateformes de streaming, semble tenace. La croissance effrénée de l'empire numérique, l'accumulation et le stockage exponentiel de données au cours des dernières décennies tend à renforcer l'image d'un monde virtuel illimité auquel aucune restriction physique ne pourrait être opposée. Néanmoins, la matérialité du numérique a déjà fait l'objet de nombreuses recherches et publications. Et pour cause, celle-ci se décline d'innombrables façons (citons par exemple : la démultiplication des terminaux utilisateurs, le développement des infrastructure afférentes, l'accumulation des e-déchets, la consommation énergétique directe et indirecte du secteur, les émissions de gaz à effet de serre et la pollution liés à la fabrication et à l'utilisation des objets numériques…).

Cette analyse s'intéresse, dans ce cadre, à la consommation de métaux[3] par l'industrie numérique et aux conséquences environnementales de ce qui s'apparente à une fuite en avant extractiviste. Bien que peu probable dans un futur proche, un retour de l'activité minière en Belgique n'apparaît plus, aujourd'hui, relever de la science-fiction. Dans le même temps, à plus de dix mille kilomètres de ses frontières, la Belgique se penche sur une potentielle exploitation minière en eaux profondes. Si certains promoteurs de l'industrie minière affirment qu'il s'agit d'une solution pour s'approvisionner en métaux nécessaires à la double transition, il s'agirait d'un dépassement de frontière inédite dans l'exploitation des ressources naturelles. Nous nous pencherons dès lors sur les polémiques qui entourent l'exploitation minière en eaux profondes et sur les nombreuses questions qui pèsent autour de l'impact environnemental et climatique d'une telle entreprise. Jusqu'ou sera-t-on prêt à descendre au nom de la « double transition » ?

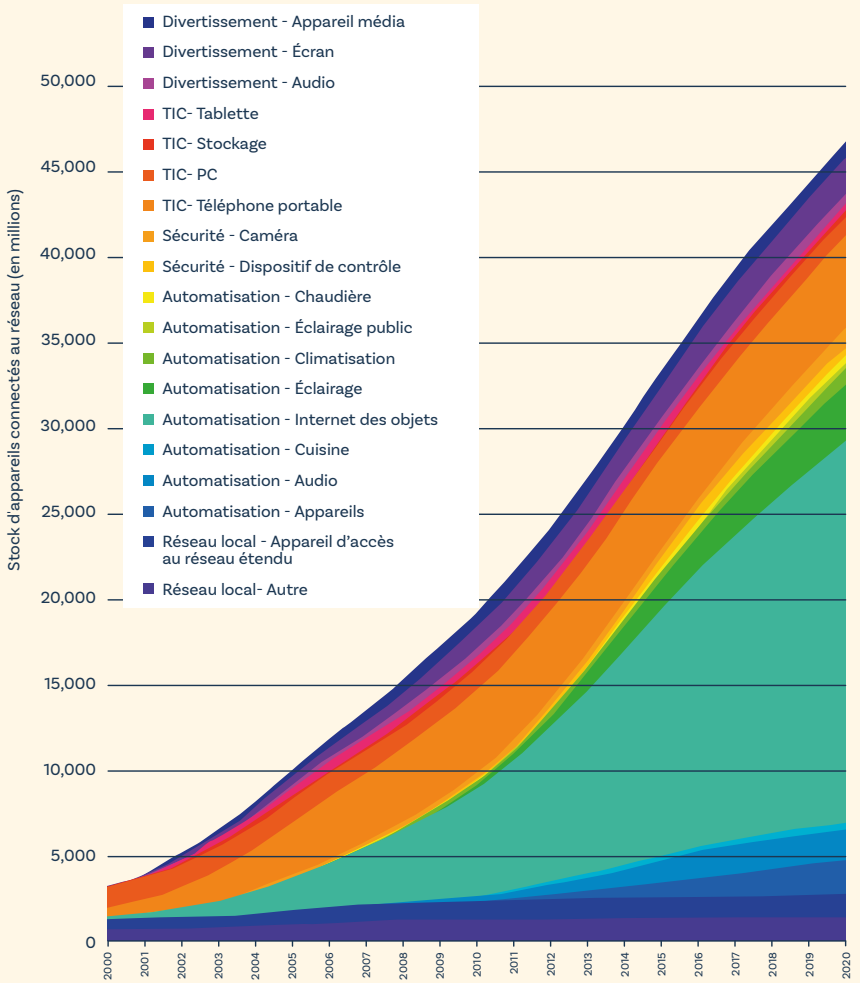
1. Avons-nous les moyens de nos ambitions ?

a. Numérisation des objets du quotidien

Malgré le développement d'appareils « multi-usages » (tels que les smartphones qui assurent les fonctions de téléphone, ordinateur portable, agenda…), les foyers comptent de plus en plus d'appareils numériques ; du thermostat « intelligent » à l'aspirateur connecté. Globalement, le nombre d'objets connectés devrait dépasser quarante-cinq milliards d'ici 2030[4]. À cette numérisation des objets du quotidien s'ajoute la problématique de l'obsolescence programmée au sens technique du terme et/ou au sens culturel, signifiant que certains appareils deviennent rapidement « passés de mode »[5]. Et cela est d'autant plus vrai que certains appareils numériques tirent leur utilité des réseaux qu'ils maintiennent entre eux. En d'autres termes, quel est l'intérêt de conserver un « bipeur » si personne, dans votre entourage, n'en possède un ?

Bien que certains appareils numériques soient bien plus efficaces énergétiquement que leurs prédécesseurs, leurs processus de fabrication se complexifient, ce qui tend *in fine* à rendre leurs cycles de vie plus énergivores. Cela s'accompagne, nous l'avons vu, d'une démultiplication des terminaux digitaux et, donc, des infrastructures afférentes. En outre, cette démultiplication des terminaux digitaux se traduit par un accroissement du trafic des données. Ainsi, les vidéos en ligne représentent 60 % du trafic global de données. Et pour cause, le visionnage de vidéos en ligne émet

Schéma 1
Évolution du stock d'appareils connectés dans le monde (2019)



Source : IEA 4E EDNA, 2019.

annuellement trois cent millions de tonnes de CO_2. Selon ces estimations, la seule consommation de vidéos pornos en ligne émet chaque année autant de CO_2 qu'un pays comme la Belgique[6].

À cette extension toujours plus importante de l'empire digital, viennent se greffer de nouveaux instruments tels que les cryptomonnaies, sans aucune valeur d'usage, particulièrement énergivores et consommateurs de matières premières. À titre d'exemple, le minage du bitcoin consommerait autant d'électricité que l'Argentine[7]. Globalement, le *think tank* Shift Project estime que les technologies digitales sont à l'origine de 4 % des émissions mondiales de gaz à effet de serre et que cette part pourrait atteindre 8 % dès 2025 (ce chiffre prend en compte leur fabrication, leur utilisation et leur durée de vie)[8].

En parallèle, la façon dont les appareils numériques et les principaux services en ligne (tels que YouTube, Gmail, les réseaux sociaux…) sont pensés, a également un impact considérable sur l'empreinte environnementale du secteur. La conception de ces services entre dans le cadre d'un « paradigme cornucopien »[9] dans le sens où ceux-ci induisent une consommation toujours plus importante de matières premières et d'énergie. Un article paru en 2016 dans la revue *Sustainability, Design and Environmental Sensibilities* pointait à ce titre que les appareils et services numériques étaient conçus pour être :

+ Personnalisés : les appareils qui étaient auparavant partagés au sein d'une famille tel que la télévision et le téléphone fixe sont désormais démultipliés par le nombre de personnes composant le foyer avec l'émergence des smartphones, tablettes, montres connectées…
+ Variés : les usagers doivent pouvoir accéder directement à un nombre illimité de services (streaming, jeu en ligne, vente et achat, visioconférence…). Ce choix illimité et disponible à

toute heure et en tout endroit induit un trafic de données toujours plus important et donc des points de relais sans cesse plus nombreux et plus performants.

+ Instantanés : accessibles avec un temps de latence réduit au minimum voire inexistant.
+ Partageables : les contenus doivent être accessibles en permanence par des tiers (par exemple, via l'utilisation du *cloud*). Cela se traduit par la nécessité de développer toujours plus d'infrastructures de stockage de type « data centers ».
+ Haute qualité : le développement permanent de la qualité des services « streamés », tels que l'apparition des vidéos 4K et désormais 8K, demande un renouvellement du hardware et augmente la consommation énergétique des services en ligne.
+ Pervasif[10] : les services en ligne doivent pouvoir être consommés à partir de n'importe quel terminal (téléphone, tablettes, télévision connectée, ...). Cela augmente, notamment, les besoins en termes de capacité de réseau.
+ L'accès continu : cela signifie que l'infrastructure doit permettre la consommation de données sans interruption et couvrir un territoire toujours plus étendu.
+ Éternel : une fois consommé, le contenu en ligne (vidéos, photos...) doit rester accessible en tout temps. Ainsi, une quantité titanesque de contenu est stockée sur des serveurs et des terminaux alors même que celui-ci ne sera peut-être plus jamais consommé.
+ Éphémère : les usagers doivent pouvoir enregistrer et télécharger du contenu en ligne sans réflexion relative à la sollicitation du réseau et à l'occupation de l'espace de mémoire de leurs terminaux même s'il s'agit d'une consommation éphémère (quelques secondes de consommation unique).

b. Un appétit insatiable pour les métaux

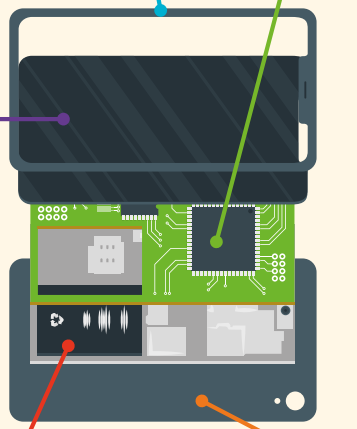
À la lecture de ce premier chapitre, il paraît clair que les métaux vont prendre une place de plus en plus importante et croissante. À taux de croissance constant, l'humanité devrait extraire en trente-cinq ans plus de métaux que tout ce qu'elle a extrait depuis l'Antiquité[11]. Si ce chiffre apparaît vertigineux, c'est parce que la tendance qui s'est dessinée au cours des dernières décennies l'est tout autant. D'une part, *la quantité* de métaux utilisés connaît une augmentation continue depuis la moitié du XXe siècle. D'autre part, *les types* de métaux utilisés se sont, eux aussi, démultipliés. En effet, jusqu'à la fin du XIXe siècle, l'humanité consommait principalement une dizaine de métaux dont du fer, du manganèse, du plomb, du zinc, du cuivre et de l'étain. Aujourd'hui, l'humanité consomme près de soixante types de métaux différents[12]. Désormais, la fabrication des appareils numériques, par exemple, requiert en moyenne plus de soixante éléments non radioactifs (sur les quatre-vingt-quatre que compte notre planète). Chacun de ces éléments est utilisé pour ses propriétés particulières (voir Schéma 1)[13]. La quantité de matières premières nécessaires, par exemple, à la fabrication d'un smartphone dépasse de très loin celle contenue dans un téléphone fixe datant de la deuxième moitié du XXe. Comme l'illustre le schéma ci-après, à lui seul, l'écran d'un smartphone comporte une dizaine d'éléments. L'Agence de l'environnement et de la maîtrise de l'énergie française, estime que chaque année en France, 62,5 millions, de tonnes de ressources sont consommées pour la fabrication et l'utilisation des appareils numériques[14].

Une fois fermés, les sites miniers peuvent continuer à polluer l'environnement

Liliane Dedryver[15] distingue deux types de métaux utilisés dans le secteur du numérique. D'un côté, ceux qui servent aux « fonctions structurelles du numérique ». Il s'agit principalement de « grands métaux » (tels que le cuivre, le plomb, le zinc, le fer...) massivement utilisés pour le maintien et le développement des infrastructures tels que les câbles et les antennes relais... De l'autre, les métaux utilisés en quantité beaucoup plus restreinte, notamment, pour la fabrication des « terminaux utilisateurs » (de type laptops, smartphones, objets connectés...) et souvent utilisés dans le cadre d'alliages complexes. Il s'agit d'éléments tels que l'indium, le néodyme, le tantale, le gallium, le germanium...[16]

Ces « plus petits » métaux utilisés dans le secteur numérique sont principalement des « sous-produits ». Cela signifie qu'ils se trouvent au sein de mines exploitées pour d'autres métaux. Par exemple, le sélénium et le tellure constituent principalement des sous-produits du cuivre, du plomb et du nickel[17]. L'exemple le plus évocateur de sous-produit est sans doute celui du cobalt dont la demande ne cesse d'augmenter, notamment, en raison du développement du secteur des batteries. Par exemple, en République démocratique du Congo, là où se situent les principales réserves de ce métal, il est exploité en tant que sous-produit du cuivre[18]. Le germanium et l'indium, pour leur part, peuvent notamment être obtenus à la suite du raffinage du zinc. Quant au gallium, il peut provenir des mines de bauxite et être séparé du minerai lors du processus de fabrication de l'aluminium. Cet état de fait explique pourquoi une part importante des métaux nécessaires aux technologies de l'information et de la communication (TIC) peuvent être perdus au cours des processus d'extraction et de transformation. Ainsi, à titre d'exemple, en moyenne, seul 15 à 20 % de l'indium contenu dans les minerais de zinc est récupéré afin de produire de l'indium

Schéma 2
Les composants d'un smartphone



Dalle tactile + vitre

In Indium	Sn Étain	Si Silicium	Al Aluminium	K Potassium

Écran

Eu Europium	Tb Terbium	Y Yttrium	
Gd Gadolinium	Ce Cérium	Tm Thulium	
La Lanthane	B Bore	Ba Baryum	
S Soufre	Mg Magnésium	Mo Molybdène	Hg Mercure

Batterie

Li Lithium	Co Cobalt	C Carbone	F Fluor
Mn Manganèse	V Vanadium	P Phosphore	Al Aluminium

Carte et composants

Ni Nickel	Pb Plomb	Sn Étain	Bi Bismuth
Au Or	Ag Argent	W Tungstène	Pt Platine
Rh Rhodium	Be Bérylium	Cu Cuivre	P Phosphore
As Arsenic	Ga Gallium	Ge Germanium	Si Silicium
Zr Zirconium	Ru Ruthénium	Nd Néodyme	F Fluor
Li Lithium	Co Cobalt	C Carbone	F Fluor
	Co Cobalt	C Carbone	F Fluor

Boîtier

Mg Magnésium	C Carbone	Sb Antimoine	Br Brome	Ni Nickel	Zn Zinc

Source : « Des métaux pas que dans les smartphones », Systext.org, mai 2020, [en ligne :] https://www.systext.org/sites/all/documents/dynamine-O2/O2_S1_Poster-A0-Schema-Smartphone_Solution.pdf

pur à 99,7%. En outre, puisque les sources d'approvisionnement sont à ce point éclatées, les raffineries achetant des concentrés de ces sous-produits sont généralement dans l'incapacité de retracer leur origine. Par ailleurs, le fait que de nombreux métaux essentiels à la fabrication des TIC soient des sous-produits d'autres grands métaux expose le secteur aux fluctuations boursières de ces derniers. Cela signifie que lorsque la spéculation boursière fait baisser le prix de certains grands métaux sur les marchés internationaux, l'attrait pour la prospection et l'extraction de ceux-ci tend à baisser. Cela a pour conséquence de limiter la production des métaux en question mais également celles de leurs co-produits[19].

c. Une chaîne d'approvisionnement sous haute tension

Certains « petits » métaux tels que le gallium et le germanium principalement exploités comme sous-produits, respectivement de l'aluminium et du zinc, ne sont pas échangés dans le cadre de marchés structurés. L'achat et la vente de ces métaux se réalise de gré à gré. Cela entretient une forte opacité autour des niveaux de production et des stocks disponibles pour ces métaux. Une situation qui pourrait mettre les fabricants du secteur *high tech* sous pression alors que la demande pour ces métaux est appelée à augmenter. D'autant plus que ces métaux sont produits et échangés en quantités très limitées, une tension en amont de la chaîne d'approvisionnement pourrait rapidement provoquer des disruptions importantes[20]. Enfin, notons que, bien qu'il existe de nombreuses mines artisanales, la mine industrielle constitue le modèle le plus développé pour l'extraction de métaux et pourvoit 88% de la production mondiale de métaux[21]. À ce titre, une série de multinationales se sont édifiées comme centrales pour le

secteur des TIC parmi lesquelles l'entreprise belge Umicore (anciennement appelée « Union-Minière » qui a notamment bâti son empire industriel en exploitant les ressources du Congo belge), la société canadienne Teck, l'américaine Indium Corp ou encore les japonais Mitsubishi et Dowa[22].

d. Les limites du recyclage

Certains pays ne disposent pas d'une industrie minière particulièrement développée mais plutôt d'infrastructures de recyclage particulièrement avancées, ce qui leur permet de devenir producteurs nets de certaines matières premières. C'est par exemple le cas de la France, de l'Allemagne, mais également de la Belgique[23]. L'entreprise d'Umicore implantée à Hoboken en Flandre est l'un des plus grands acteurs du secteur du raffinage et du recyclage des métaux précieux[24]. Le développement du recyclage des métaux constitue un élément essentiel pour limiter l'impact de l'industrie minière sur l'environnement. Néanmoins, cela ne suffira pas à compenser la croissance annuelle moyenne de la demande qui s'établit autour de 3 % par an pour de grands métaux tels que le cuivre ou le fer, voire autour de 6 % pour d'autres plus « petits » métaux[25]. Olivier Vidal, directeur de recherche au CNRS, note à ce titre que « *si l'humanité n'est pas capable de réguler sa consommation de ressources en adoptant des pratiques plus économes et en acceptant l'idée que la croissance éternelle à taux constant est une utopie, la limite de notre monde fini s'imposera d'elle-même. Elle s'imposera par atteinte d'un niveau de saturation, par manque d'énergie ou de ressources, par dégradation de notre environnement, mais elle s'imposera. À ce moment-là, les pays riches passeront de l'illusion de croissance infinie à la réalité de la stagnation ou de la décroissance imposée, et ce passage sera sans aucun doute très douloureux s'il n'a pas été anticipé* »[26].

Tableau 1
Aperçu des éléments utilisés pour la fabrication d'appareils numériques

Élément	Symbole	Usage dans les TIC
Antimoine	Sb	Éléments d'alliage dans les batteries au plomb
Bérillyum	Be	Contacts électriques, les satellites de communication
Bore	B	Dopants dans les semiconducteurs
Brome	Br	Retardateurs de flamme dans les boîtiers de téléphone portable
Césium	Cs	Composants photoélectriques
Chrome	Cr	Alliages
Cobalt	Co	Batteries rechargeables
Cuivre	Cu	Connexions électriques
Gallium	Ga	Circuits intégrés, LED, appareils photovoltaïques
Germanium	Ge	Fibre optique, technologie infrarouge
Or	Au	Composants microélectroniques, connexions électriques
Graphite	C	Batteries rechargeables
Éléments de terres rares lourdes	p. ex. : Dy, Tb…	Aimants utilisés dans les micros, les hauts-parleurs, les écrans…
Hélium	He	Gaz de protection
Indium	In	Écrans
Éléments de terres rares légères	p. ex. : Pr, Nd…	Aimants utilisés dans les micros, les hauts-parleurs, les écrans,…
Plomb	Pb	Soudures
Lithium	Li	Batteries rechargeables
Magnésium	Mg	Alliages pour les coques de téléphone portable
Manganèse	Mn	Batteries rechargeables

Nickel	Ni	Micros, connexions électriques
Niobium	Nb	Alliages
Métaux du groupe platine	Pd, Pt, Rh, Ru, Os, Ir	Alliages
Sélénium	Se	Appareils photovoltaïques
Silicium	Si	Circuits intégrés
Argent	Ag	Composants microélectriques
Tantale	Ta	Condensateurs
Tellure	Te	Appareils photovoltaïques
Étain	Sn	Soudures sans plomb
Tungstène	W	Matériaux diélectriques (isolants électriques), filaments
Vanadium	V	Batteries rechargeables

Source : Conférence des Nations unies sur le commerce et le développement, op. cit., p.9.

e. Le mythe des "métaux rares"

D'après Aurore Stephant, ingénieure géologue minière et membre de l'ONG SystExt, le fait que certains métaux seraient « *plus rares* » que d'autres relèverait d'une « *certaine mythologie* »[27]. En effet, à l'exception de quelques éléments (comme l'aluminium, le fer, le magnésium, le titane et le manganèse), la grande majorité des métaux ne sont que peu concentrés dans le sous-sol. Cela signifie qu'il est nécessaire d'excaver de grandes quantités de roches pour n'obtenir qu'une petite quantité du minéral recherché. Ainsi, la plupart des gisements de métaux présentent des teneurs très faibles, autour de 1 voire 0,1 %[28]. À titre d'exemple, dans les salars[29], les teneurs en lithium s'élèvent en moyenne entre 0,05 et 0,15 %. Pour le platine, les gisements exploités présentent une teneur moyenne entre 0,0003 % et 0,00015 %[30] En outre, il convient de souligner que plus les gisements sont exploités, plus la teneur en métal de ce dernier tend à baisser. Cela signifie qu'une fois les « gros filons » exploités, il devient nécessaire d'extraire de plus en plus de roches pour obtenir de moins en moins de métal. En d'autres termes, il faut consommer de plus en plus d'énergie et générer de plus en plus de déchets pour un rendement toujours plus faible[31].

2. "Double transition", même extractivisme

a. Explosion de la demande

Comme mentionné plus haut, la demande en métaux, poussée par la transition énergétique et la digitalisation, devrait croître très rapidement et parfois, dans des proportions très importantes. Dans ce cadre, le secteur de la transition énergétique et le secteur numérique entrent en compétition pour l'approvisionnement de certaines matières premières qu'il s'agisse de « petits » ou de « grands métaux ». Et pour cause, l'Agence internationale de l'énergie (AIE) estime que se conformer à l'Accord de Paris de la COP 21[32] signifierait une augmentation de 40 % de la demande pour le cuivre et les éléments de terres rares, de 70 % pour le nickel et de 90 % pour le cobalt et pour le lithium. Par exemple, une installation éolienne terrestre nécessite, en effet, neuf fois plus de minerais par puissance installée qu'une centrale au gaz. Et cette tendance se vérifie également pour la fabrication de champs photovoltaïques[33].

En parallèle, la décarbonation de l'économie européenne passe par son électrification et cela suppose de nouvelles infrastructures et donc, plus de matières premières. En 2017, le réseau électrique français comptait cent septante mille tonnes de cuivre et cette part devrait croître de trente mille tonnes au cours de la première moitié de la décennie 2020[34]. En Belgique, Elia, le gestionnaire du réseau national de transport d'électricité à haute tension, a pour ambition de créer une ligne à haute tension longue de plus de quatre-vingts kilomètres d'Avelgem à Courcelles en Province du Hainaut[35]. L'objectif est de permettre le transport d'électricité, notamment, en provenance du parc éolien en mer du Nord. Ce projet – qui suscite une levée de boucliers tant dans le chef des habitants que dans celui de certains bourgmestres concernés[36] – constitue une parfaite illustration de la « matérialité » de la transition énergétique et de notre consommation électrique croissante.

b. L'exemple des véhicules électriques

Les véhicules électriques (VE), quant à eux, constituent un exemple éclairant de conjonction entre transition numérique et énergétique. En effet, d'une part ces véhicules ne carburent pas à l'énergie fossile et, d'autre part, ils intègrent toute une série d'options digitales. L'Union européenne a, dans le cadre du Pacte vert pour l'Europe, tranché en faveur d'une interdiction de la vente de véhicules thermiques neufs au sein de l'UE d'ici 2035[37]. Or, la fabrication d'un VE exige six fois plus de minerais que celle d'un véhicule conventionnel. Par exemple, le secteur de l'acier inoxydable devrait céder sa place de premier consommateur de nickel aux secteurs des VE et des batteries dès 2040[38]. Le développement à grande échelle des véhicules électriques ajoutera également une pression supplémentaire sur la demande de cuivre. Et pour cause, une augmentation de 5 à 10 % du parc automobile électrique se traduirait par une augmentation de la consommation de cuivre de l'ordre de quatre millions de tonnes d'ici 2030. Parmi ces quatre millions de tonnes, une « seulement » serait dédiée aux infrastructures, au réseau et aux dispositifs de recharge et de stockage. Les trois millions de tonnes restantes seraient utilisées pour la fabrication des véhicules eux-mêmes[39]. Or, la Commission européenne souligne que la hausse de la demande en métaux se heurtera aux limitations de l'offre[40]. Ainsi, les capacités extractives de l'industrie du cobalt ne permettraient pas de répondre à plus de 50 % de la demande anticipée. Et la tendance se confirme pour d'autres matières premières et, notamment, les terres rares utilisées, tant dans les technologies de transition que dans les TIC[41]. De quoi remettre en perspective les estimations de la Commission européenne qui prévoient trente millions de VE au sein de l'UE d'ici 2030[42]. (on comptait 1,9 millions de véhicules 100 % électriques en 2021[43]).

Comme l'illustre le graphique ci-après, la Commission européenne estime que, d'ici 2030, *les batteries nécessaires à la mobilité électrique* pourraient nécessiter, à elles seules, dix fois plus de lithium que tout ce que l'UE consomme (tous secteurs confondus). Et d'ici 2050, celles-ci pourraient solliciter jusqu'à quarante fois plus de lithium que ce qui est actuellement consommé, tous secteurs confondus au sein de l'UE. Et cette tendance se vérifie également pour d'autres métaux tels que le graphite, le cobalt, le nickel et le manganèse. À cela s'ajoute encore le développement à grande échelle des dispositifs d'énergie renouvelable, la multiplication des data centers, la digitalisation des objets du quotidien, le développement d'infrastructures adéquates, l'électrification de l'outil productif…

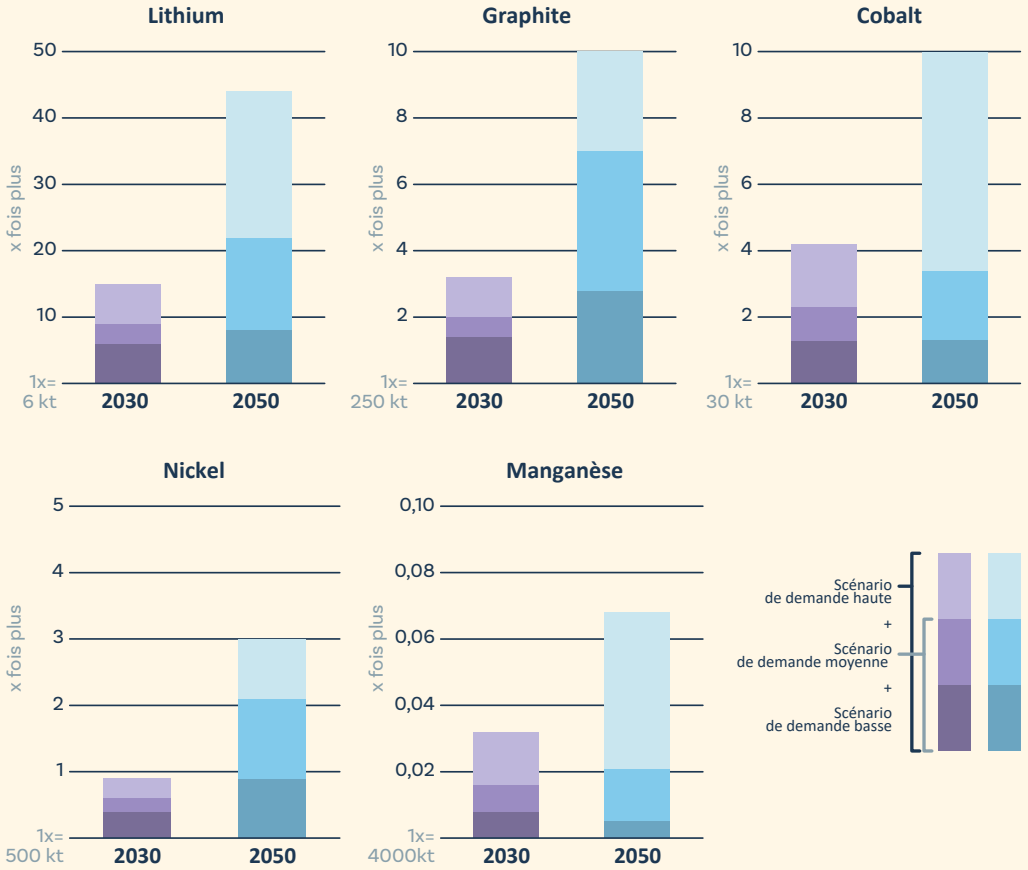
3. La relance minière en Europe

Le 16 mars 2023, la Commission européenne a publié le *Critical Raw Material Act* (« législation sur les matières premières critiques »). Cette initiative se compose d'une proposition de règlement[44] et d'une communication[45]. Elle s'inscrit dans le cadre, plus large, du Pacte vert pour l'Europe qui vise à atteindre la neutralité carbone d'ici 2050[46]. Concrètement, il s'agit d'une tentative de réponse à un double problème : d'une part, l'extrême dépendance de l'UE à l'égard des pays tiers pour toute une série de matières premières et, d'autre part, le fait qu'une poignée de pays – au premier chef, la Chine – détiennent un quasi monopole sur la production et la transformation de celles-ci. En particulier, cette initiative de la Commission vise les matières premières (non énergétiques et non agricoles) considérées comme « stratégiques » et « critiques » par l'UE. Les matières premières stratégiques sont celles dont la production pourrait ne pas suivre l'augmentation de la demande prévue dans le cadre des transitions énergétique et digitale. Les matières premières critiques, quant à elles, reprennent les seize matières premières identifiées comme stratégiques plus vingt autres dont une pénurie ou une interruption dans la chaîne d'approvisionnement pourrait constituer une menace pour l'économie européenne[47].

Dans le détail, la proposition prévoit que, d'ici 2030, la *production* communautaire de matières premières stratégiques équivale à 10 % de la demande intérieure de l'UE. En d'autres termes, la proposition de règlement appelle à relancer massivement l'activité minière en Europe. Elle vise également à augmenter les capacités européennes en termes de *transformation* pour répondre à, au moins, 40 % de la demande intérieure. Enfin, le *recyclage* devrait, lui aussi, considérablement augmenter et satisfaire 15 % de la demande européenne. La Commission entend ainsi diversifier son approvisionnement en matières premières stratégiques. Pour ce faire, l'exécutif européen propose de développer une politique d'identification de projets « stratégiques » d'extraction, de transformation et de recyclage au sein de l'UE ou de pays tiers. Pour identifier ces projets, la Commission devrait s'appuyer sur le soutien d'une institution *ad hoc*, le European Critical Material Board dont la composition reste à définir.

Quoiqu'il en soit, les projets identifiés comme « stratégiques » devront tendre vers le respect d'une série de critères notamment en termes de faisabilité technologique ainsi que de « durabilité sociale et environnementale ». Si ces dispositions laissent penser que les impacts environnementaux et sociaux seront étudiés en profondeur avant le lancement de projets extractifs, d'autres éléments présents dans la proposition législative trahissent une réalité beaucoup plus contrastée. Et pour cause, le paragraphe dix-neuf souligne que les projets identifiés comme stratégiques

Schéma 3
Consommation supplémentaire de matières premières uniquement pour les batteries nécessaires à la mobilité électrique en 2030/2050 par rapport à la consommation actuelle de ces matières premières dans l'UE, tous secteurs confondus



Lecture du graphique : L'axe des ordonnées pour 2030 et 2050 indique la demande supplémentaire de matériaux pour les batteries nécessaires à la mobilité électrique par rapport à la consommation moyenne totale de l'UE sur la période 2012-2016. Trois scénarios sont envisagés par la Commission européenne : un scénario « demande basse », un scénario « demande moyenne » et un scénario « demande haute ». Ceux-ci correspondent aux différents coloris des graphes. Le scénario « demande moyenne » est considéré « le plus probable et le plus crédible » par la Commission.
Source : Critical Raw Materials for Strategic Technologies and Sectors in the EU. A Foresight Study, Bruxelles : Commission européenne et Joint Research Center, 2020, 98 p.

devront être considérés comme « servant l'intérêt public ». De ce fait, la Commission estime que « *Les projets stratégiques qui ont une incidence négative sur l'environnement (…) peuvent être autorisés lorsque l'autorité compétente chargée de l'octroi des autorisations conclut, sur la base d'une évaluation effectuée au cas par cas, que l'intérêt public que sert le projet l'emporte sur ses incidences, pour autant que toutes les conditions pertinentes énoncées dans ces directives soient remplies* »[48]. On peut donc imaginer que des l'extraction de métaux nécessaires à la transition énergétique entreraient dans ce cadre.

En outre, pour garantir des octrois de permis rapides, la Commission estime qu'il est nécessaire de « rationaliser » les évaluations, notamment, environnementales. Dans le même sens, la proposition de règlement insiste sur la nécessité de résoudre rapidement les éventuels litiges concernant l'octroi d'un permis pour le lancement d'un projet identifié stratégique (§ 21). Cela pose de nombreuses questions concernant la façon dont ces litiges seront pris en charge et, surtout, concernant les possibilités qui seront offertes aux riverains et citoyens pour s'opposer au lancement d'un projet minier. D'autant plus que la Commission estime que l'octroi d'un permis pour un projet extractif ne devrait pas excéder deux ans (§ 23).

Dans sa communication qui accompagne la proposition de règlement, la Commission propose même d'inclure certaines activités extractives et de raffinage dans la taxonomie européenne des investissements durables[49]. Celle-ci fonctionne comme un label européen pour les « investissements verts ». Elle vise donc à encourager les investisseurs institutionnels (fonds spéculatifs, banques d'affaires…) à rediriger leurs capitaux vers des activités moins néfastes pour l'environnement. En d'autres termes, investir dans un

projet minier en Europe pourrait constituer un « investissement durable » au regard de la législation européenne si ces minerais servent, par exemple, à la fabrication de véhicules électriques.

De plus, la transparence à l'égard des citoyens européens est loin d'être garantie puisque le document de *reporting* à charge des États membres concernant l'exploration, le suivi et les stocks pourraient être « confidentiels ou à diffusion restreinte » (§ 57). La proposition législative devra néanmoins passer par le Conseil et le Parlement avant d'être adoptée. Bien que cette proposition réponde à une demande du Conseil et soit fortement soutenue par le Commissaire au Marché intérieur, il semble difficile d'imaginer que le texte soit définitivement adopté avant la fin de cette législature. Nous l'avons vu, celui-ci comporte, en effet, de nombreuses dispositions extrêmement sensibles[50].

Il convient néanmoins de s'interroger sur les incidences que ce règlement pourrait avoir en Belgique s'il venait à être adopté en l'état. Et pour cause, la Commission insiste sur l'intérêt que présentent les anciens sites industriels et, notamment, les anciens sites de traitements de déchets miniers. À ce titre, l'exemple de l'ancienne région minière de La Calamine et Plombières apparaît intéressant. Au XIXe siècle, cette région située à l'est de la Belgique, constituait la principale source de production du zinc et de plomb dans le monde. C'est notamment avec le zinc de La Calamine qu'ont été construits les toits des immeubles haussmaniens de Paris. L'exploitation des mines de zinc et de plomb s'est arrêtée au cours de la première moitié du XXe siècle, en partie, à cause des inondations régulières des galeries. Les mines ont, depuis lors, été rebouchées. Mais tel qu'évoqué plus haut, la demande croissante en métaux a ravivé l'appétit de certains « investisseurs ». Et pour cause, les mines de plomb et de zinc renfermeraient encore une série d'autres métaux fondamentaux pour le développement des nouvelles technologies. Le sous-sols de La Calamine et Plombières disposerait, en effet, encore de larges quantités de zinc mais également d'autres métaux tels que le germanium, le gallium et l'indium. Autant de petits métaux nécessaires à la fabrication d'écrans tactiles, de fibres optiques, de capteurs optoélectroniques… Dans ce cadre, en 2018, la société Walzinc, basée à Wavre, a soumis à la Région wallonne une demande de permis pour une campagne d'exploration. Le projet s'est heurté à une farouche opposition des riverains et la demande a finalement été déboutée par les pouvoirs publics wallons.[51]

En effet, la législation relative à l'extraction minière relève de la compétence des États membres et, plus précisément, des Régions en ce qui concerne la Belgique. Suite à la demande de permis de Walzinc les autorités wallonnes ont lancé une actualisation du code minier régional, le Code de gestion des ressources du sous-sol. D'après un article paru dans le quotidien *l'Écho* en décembre 2018, le projet prévoirait l'instauration d'un permis d'environnement, une enquête publique préalable à l'octroi d'un permis d'exploration et d'exploitation et une série d'obligations de suivi lors de la fermeture du site minier. Si ce projet d'actualisation du code minier wallon prévoit l'inscription de nouveaux garde-fous environnementaux et démocratiques, il signifie également que les autorités wallonnes ne seraient pas réfractaires à l'idée d'un retour de l'industrie minière dans la Région[52].

4. Une industrie particulièrement polluante

Nous l'avons vu, la fabrication de l'équipement numérique constitue une part importante de l'empreinte carbone du secteur digital. Et cette part est d'autant plus importante lorsqu'il s'agit de terminaux offrant de nombreuses fonctionnalités tels que les smartphones pour lesquels 80 % de l'empreinte carbone est réalisée avant même sont utilisation[53]. Intéressons-nous, à ce titre, à l'amont de la chaîne de production c'est-à-dire à l'extraction des matières premières nécessaires à la fabrication des TIC.

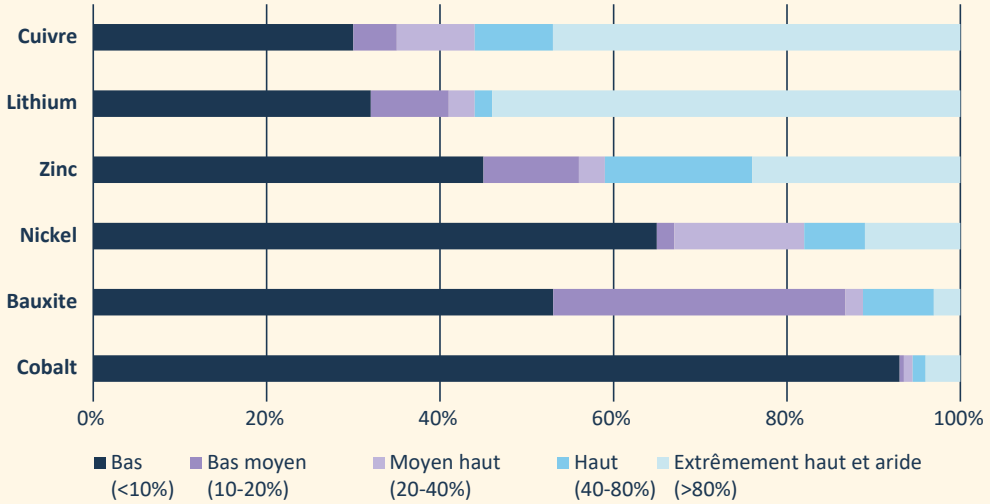
Et pour cause, les activités minières causent des dommages environnementaux considérables et ce, dès l'ouverture de la mine jusqu'à sa fermeture[54]. Tout d'abord, les mines s'étendent sur d'importantes surfaces, ce qui nuit inévitablement au biotope. En outre, la poussière émise par le site d'exploitation peut contenir de nombreuses particules telles que du plomb ou de l'arsenic. Quant à l'empreinte carbone, l'industrie minière serait à l'origine de 4 à 7% des émissions globales de gaz à effet de serre[55]. Comme mentionné plus haut, les teneurs en métaux dans le sous-sol sont, en l'état, généralement faibles ce qui nécessite d'excaver des quantités de roches toujours plus importantes. Cela signifie également que les processus de traitement de transformation sont longs et nécessitent de nombreux intrants chimiques. En conséquence, l'activité extractive génère énormément de déchets. Or, les résidus miniers peuvent être hautement polluants et leur stockage pose de nombreux risques pour l'environnement. D'autant plus que leur quantité croît considérablement, corrolairement à la croissance de l'activité minière. Au total, c'est plus de cent millions d'hectares sur Terre qui sont recouverts par des déchets miniers.

De plus, afin de pouvoir être utilisés par l'industrie du numérique et des technologies vertes, certains métaux requièrent une extrême pureté. Pour atteindre un tel niveau, des quantités considérables de matière doit être extraite du sous-sol et le processus de transformation s'avère extrêmement lourd et complexe. En parallèle, certaines mines nécessitent des pompes pour assécher

le site d'exploitation et accéder au minerais. Dans le même temps, les processus de transformation et de concentration nécessitent d'importantes quantités d'eau. Cela mène l'Agence internationale de l'énergie à souligner la vulnérabilité de l'industrie minière à l'égard du dérèglement climatique. En effet, tel que l'illustre le graphique ci-dessous, plus de la moitié de la production de cuivre et de lithium se situe dans des zones exposées au stress hydriques. En outre, il apparaît que certaines ressources nécessaires à la double transition telles que le lithium et les éléments de terres rares nécessitent en moyenne plus d'eau que l'extraction et le traitement d'autres matières premières[56].

Il convient également de souligner que l'activité minière relâche d'importantes quantités d'eaux usées. Même s'il existe généralement des limites légales concernant les concentrations de déchets contenues dans les eaux rejetées, l'effet cumulatif peut exercer un stress pour l'environnement. De plus, il arrive que les digues qui retiennent de larges quantités d'eau contaminée cèdent. Cela génère un déversement torrentiel d'eaux polluées dans le biotope. Si une étude[57] commandée par la commission des pétitions du Parlement européen parle de « situations exceptionnelles », les exemples sont pourtant loin de manquer. Et pour cause, chaque année, trois à sept accidents de ce type sont répertoriés dans le monde (il s'agit probablement d'une sous-estimation puisque les accidents dans les mines artisanales demeurent très peu signalés). Et cela ne concerne pas que les pays en développement. En Europe, plusieurs digues artificielles se sont effondrées au cours des dernières années notamment en Espagne en 1998[58], en Roumanie en 2000[59] ou encore en Hongrie en 2010[60]. Globalement, la pollution de l'eau par l'industrie minière est difficile à quantifier. Néanmoins, une étude menée en 2013 portant sur quarante mines aux USA a démontré qu'elles généraient quatre-vingt milliards de litres d'eau contaminée chaque année[61].

Schéma 4
Part du volume de production par niveau de stress hydrique (2020)



Source : Agence internationale de l'énergie, op. cit.

Enfin, il convient de noter qu'une fois fermés, les sites miniers peuvent continuer à polluer l'environnement durant des décennies voire des siècles[62]. Par exemple, en Chine, l'exploitation minière aurait déjà érodé environ 40 000 km² de terres et l'espace occupé par des mines abandonnées augmentent chaque année d'environ 330 km². Aux États-Unis, 550 000 mines abandonnées ont été identifiées et parmi celles-ci plus de cent mille poseraient de sérieux risques environnementaux[63]. Les terrains miniers abandonnés présentent, en effet, généralement une carence en éléments nutritifs pour les plantes, des taux importants de pollution aux produits chimiques toxiques ainsi qu'une forte altération de la qualité des sols[64].

Toutes ces considérations conduisent les auteurs du rapport du Parlement européen à s'interroger sur la faisabilité de relance minière en Europe : « *Dans la perspective de la réalisation des objectifs de la transition verte, le nombre croissant de conflits et d'oppositions aux projets miniers pourrait devenir un obstacle majeur. Cette situation a également amené certaines personnes à s'interroger sur le réalisme des plans d'exploitation minière* »[65]. D'autant plus qu'à cela s'ajoute les émissions de gaz à effet de serre, la pollution et la consommation de ressources liée à la transformation de ces métaux en produits consommables par l'industrie du numérique et énergétique. À titre d'exemple, TSMC, l'un des principaux fabricants de semi-conducteurs au monde basé à

Taïwan consomme environ deux cent mille tonnes d'eau chaque jour, alors même que le pays est de plus en plus confronté aux sécheresses[66]. Il semble difficilement imaginable que de telles activités soient « relocalisables » au sein de l'UE et, plus fondamentalement, qu'elles puissent répondre à la croissance effrénée de la demande. Néanmoins, le sous-sol n'est pas l'unique objet de convoitise des industries minières. Depuis quelques années déjà, les besoins croissants en métaux ont fait naître un regain d'intérêt pour l'exploitation minière en eaux profondes. Une nouvelle frontière dans l'exploitation des ressources naturelles qui semble particulièrement intéresser la Belgique.

5. Exploiter les fonds marins pour sauver la planète ?

a. Quelques notions et définitions

Le *Deep sea mining* ou l'extraction minière en eaux profondes en français consiste comme son nom l'indique à puiser dans les fonds marins afin d'y extraire des matières premières. Les fonds marins sont, en effet, riches en métaux, notamment, en cobalt, nickel, cuivre et manganèse, particulièrement recherchés dans le cadre de la transition énergétique et de la digitalisation. Plus précisément, le *Deep sea mining* recouvre principalement l'exploitation de trois types de ressources :

- Les nodules polymétalliques qui se situent entre quatre mille et 6500 mètres sous le niveau de la mer. Il s'agit de concrétions lovées dans les fonds marins mesurant entre deux et quinze centimètres de diamètre. Présents partout sur la planète mais surtout concentrés dans l'océan Pacifique, ils contiennent notamment du manganèse, du fer, du nickel, du cuivre, du cobalt et des terres rares[67].
- Les encroûtements cobaltifères qui se trouvent entre quatre cents et quatre mille mètres de profondeur. Il s'agit d'agrégats rocheux riches en cobalt, en platine et potentiellement en titane, en nickel, en cérium, en thallium, en tellure, en zirconium, en tungstène en bismuth et en molybdène. Les principales ressources se situent en Polynésie dans les eaux territoriales françaises[68].
- Les gisements de sulfures polymétalliques localisés entre mille et quatre mille mètres de profondeur. Il s'agit de monticules pouvant atteindre septante mètres de hauteur et potentiellement très riches en métaux, notamment, en cuivre, en zinc et en cobalt. Ceux-ci seraient principalement situés dans l'océan Pacifique[69].

Une entreprise doit être parrainée par un État membre de l'AIFM

D'après, Gerard Barron[70], PDG de The Metals Company – une société canadienne spécialisée dans l'exploitation minière en eaux profondes –, le *Deep sea mining* serait « *le moyen le plus simple de résoudre le problème du changement climatique* »[71]. D'après ce dernier, exploiter les nodules polymétalliques serait « *aussi simple que d'aspirer des balles de golf* ». Même son de cloche du côté de l'entreprise belge Global Sea Mineral Resource (GSR), une filiale du groupe DEME créée spécialement pour l'exploitation minière en eaux profondes.[72] Son directeur général estime que « le *plus grand risque qui pèse actuellement sur les océans est le réchauffement climatique* ». Pour lui, « *la solution peut être trouvée dans les fonds marins, où il existe un gisement unique qui fournit les minéraux dont nous avons besoin pour les infrastructures d'énergie propre* ».[73]

Concrètement, l'exploitation minière sous-marine est déjà une réalité. Cela se déroule néanmoins à des profondeurs relativement faibles et dans les eaux relevant de la souveraineté nationale des États. C'est par exemple, le cas au large de la Namibie et de l'Indonésie. En Europe également, des entreprises minières entendent profiter de ces richesses situées le long des États côtiers. À titre d'exemple, une entreprise minière suédoise a déposé un permis d'exploration pour une potentielle exploitation de nodules polymétalliques au sein de la mer Baltique.[74] En parallèle, l'Espagne et le Portugal ont, eux aussi, fait part de leur intérêt pour une potentielle exploitation minières au sein de leurs plateaux continentaux.[75] Néanmoins, l'exploitation minière en eaux profondes s'avère bien plus complexe. Juridiquement, tout d'abord, puisque la Convention des Nations unies sur le Droit de la Mer (CNUDM)[76] prescrit que les ressources localisées dans les eaux internationales constituent un patrimoine commun de l'humanité. Cela signifie qu'une potentielle exploitation de ces ressources doit bénéficier à « tous les peuples sans aucune forme de discrimination ». Dans ce cadre, les fonds marins de la « Zone » (c'est-à-dire les fonds marins et océaniques au-de-là des limites nationales) relèvent de l'Autorité internationale des fonds marins (AIFM) composée de cent soixante-sept États membres dont la Belgique[77].

Concrètement, afin de bénéficier d'un permis d'exploration pour l'extraction minière en eaux profondes, une entreprise doit être parrainée par un État membre de l'AIFM. Les permis octroyés peuvent s'étendre sur un périmètre pouvant atteindre jusqu'à 150 000 km². Depuis 2001, au moins trente contrats d'exploration ont été délivrés par l'AIFM. Et au total, ce sont 1,5 million de km² répartis entre les océans Pacifique, Atlantique et Indien qui sont concernés par ces permis. Et parmi ceux-ci figure celui de l'entre-

prise GSR, parrainée par l'État belge. Ce parrainage permet à GSR de mener des tests d'exploration dans les fonds marins de la zone de Clarion Clepperton situé dans l'océan Pacifique. Cette zone située entre Hawaï et le Mexique s'étend sur 4,5 millions de km^2. Elle serait particulièrement riche en métaux. La zone d'exploration octroyée en 2013 à GSR recouvre, pour sa part, 77 000 m^2, soit 2,5 fois la superficie du territoire belge[78].

b. L'industrie accélère le tempo

En 2013, faisant suite à la sollicitation de l'entreprise GSR, le gouvernement belge a adopté une législation[79] encadrant le processus de parrainage d'une entreprise pour l'exploration minière en eaux profondes[80]. La loi belge reporte l'ensemble des responsabilités sur le contractant notamment, en cas de dommages pour l'environnement. Néanmoins, Klaas Willaert, Professeur en droit de la Mer à l'Université de Gand, rappelle que l'État parrain est tenu de veiller à ce que l'entreprise parrainée se conforme à ses obligations, définies dans la CNUDM[81]. Une considération d'autant plus importante qu'il revient à GSR de contrôler les impacts de ses propres activités sur l'environnement et d'en faire rapport au gouvernement.

Si pour l'instant, seuls des permis d'exploration ont été délivrés, les États et les entreprises minières pourraient commencer à solliciter un permis d'exploitation effective auprès de l'AIFM dès juillet 2023. En effet, l'île de Nauru (située dans l'océan Pacifique et qui parraine la société *Nauru Ocean Resources*, une filiale de l'entreprise The Metals Company, voir plus haut), a soumis à l'AIFM une demande d'exploitation effective en juin 2021. Cette démarche a automatiquement enclenché la règle dite des « deux ans ». Celle-ci implique que l'AIFM doit rédiger un cadre réglementaire encadrant les exploitations minières dans la Zone d'ici le 9 juillet 2023[82]. Concrètement, il s'agit d'une large négociation multilatérale sur base du projet de règlement préparé par la Commission juridique et technique[83].

Étant donné la complexité d'un tel processus, notamment, en ce qui concerne le partage des recettes d'une ressources issue du patrimoine mondial de l'humanité, il apparaît, en l'état, peu probable que l'échéance initiale soit respectée[84]. Le réseau international de chercheurs *Deep-Ocean Stewardship Initiative* a, à ce titre, publié un communiqué de presse le 29 juin 2021 affirmant que « *le déclenchement de la règle des deux ans ne permettra pas à une grande partie de la recherche scientifique pertinente d'être achevée, communiquée et prise en compte, empêchant toute prise de décision critique et fondée sur des données scientifiques* ». Le réseau propose d'étendre la période d'observation des impacts, au moins, durant la Décennie des Nations unies pour les sciences océaniques au service du développement durable qui se déroule de 2021 à 2030[85].

Dans ce contexte, le gouvernement belge, lui aussi, doit émettre une proposition de loi nationale pour encadrer un potentiel parrainage de l'exploitation minière en eaux profondes. Le projet de loi devrait, en principe, être présenté à la Chambre au cours de l'été 2023. Or, rien ne semble moins sûr. Le 9 mars 2023, les présidents de six partis politiques (Écolo, Défi, les Engagé·e·s, Groen, le PS et le PTB) ont co-signé une lettre ouverte dans le journal Le Soir appelant à un moratoire sur la question[86]. En l'état, le site web du Ministère des Affaires étrangères apporte quelques éléments concernant ce qui pourrait se trouver dans le texte de loi[87]. Celui-ci indique que « *la Belgique applique strictement le principe de précaution. Il ne peut y avoir d'exploitation des fonds marins sans un accord sur un ensemble de règles et de réglementations qui préviennent les dommages significatifs à la biodiversité des océans et aux écosystèmes marins* ». Concrètement, la Belgique émettrait trois conditions principales à l'autorisation de l'extraction minière en eaux profondes. Premièrement, l'établissement d'un cadre réglementaire « solide et respectueux de l'environnement » par l'AIFM. Notons, à ce titre, qu'en 2023 la Belgique siège au Conseil de l'AIFM et peut donc jouer un rôle clé dans l'élaboration d'un cadre réglementaire pour l'exploitation des ressources de la Zone. Deuxièmement, la Belgique souhaite de nouvelles recherches scientifiques sur les impacts de l'extraction minière en eaux profondes et, enfin, la « *prise en compte de la protection de l'océan* »[88].

“Un cadre réglementaire solide et respectueux de l'environnement”

Dans ce cadre, nous pouvons nous interroger sur le fait que, malgré les prises de positions de certains partis siégeant au gouvernement fédéral, la Belgique refuse de se positionner officiellement en faveur d'un moratoire. Parmi les pays en faveur de ce moratoire, nous pouvons citer le Chili, l'Allemagne, l'Espagne, la Nouvelle-Zélande, le Costa Rica, une alliance de pays insulaires du Pacifique tels que Paulu, les îles Fidji et la Micronésie[89] et, plus récemment, la France[90]. Le Parlement européen s'est lui-même positionné en faveur d'un moratoire (§ 184)[91]. Dans le même temps, plus de deux cents parlementaires originaires de près de cinquante pays – dont quelques députés belges – ont également signé un appel à un moratoire[92].

c. L'AIFM sous le feu des critiques

L'AIFM dispose d'un organe autonome et opérationnel dénommé l' « Entreprise ». L'objectif de cet organe n'est autre que le développement d'une activité minière en eaux profondes propre à l'AIFM. Par ailleurs, l'Entreprise pourrait, outre ses activités minières, développer des activités de transformation et de distribution des matières premières collectées. Une entreprise privée canadienne Nautilus Minerals Inc. a soumis une demande de *joint-venture* avec l'Entreprise en 2012. Six ans plus tard, l'État polonais a également soumis une demande similaire. Néanmoins, aucune de ces propositions n'a, pour l'instant abouti[93]. Quoi qu'il en soit, le fait que l'AIFM – l'agence chargée de protéger les fonds marins de la Zone et d'encadrer l'exploitation de ses ressources – soit, elle-même, un potentiel acteur industriel et commercial mène les organisations environnementales à s'interroger sur son indépendance. Arlo Hemphill, responsable de la campagne sur les océans pour Greenpeace déclarait, à ce titre, au quotidien américain *LA Times* qu' « *il est extrêmement préoccupant que l'AIFM soit chargée de gérer une entreprise qu'elle est également chargée de réglementer* »[94].

L'article paru en avril 2022 mettait également en cause l'indépendance du secrétaire général de l'AIFM, Michael Lodge, un avocat britannique élu par l'Assemblée le 21 juillet 2016.[95] Le quotidien américain va même jusqu'à le qualifier « d'allié des compagnies minières ». Le *LA Times* rapportait, en effet, que l'apparition du secrétaire général dans le cadre d'une vidéo promotionnelle de l'entreprise minière Deep Green a interpellé jusqu'à sa propre administration. Dans le même temps, plusieurs États membres tels que l'Australie, le Royaume-Uni et le Mexique auraient émis des critiques concernant le manque d'exigence de l'AIFM en ce qui concerne les études d'impacts environnementaux réalisées par les opérateurs miniers disposant de permis d'exploration. D'anciens employés de l'Agence onusienne ont également pointé un manque de diligence dans le contrôle des entreprises intéressées par l'exploitation minière en eaux profondes. Des critiques balayées par le secrétaire général de l'AIFM qui regrette « *un absolutisme et un dogmatisme environnementaux croissants, à la limite du fanatisme* »[96].

> **"Un absolutisme et un dogmatisme environnementaux à la limite du fanatisme"**
> **Michaël Lodge,** secrétaire général de l'AIFM

Enfin, l'AIFM est également critiquée pour son manque de transparence. À ce titre, il convient de souligner que le secrétaire général négocie lui-même « personnellement » avec les compagnies minières. Un e-mail datant de 2017 et révélé par la presse américaine faisait état d'une communication entre Barron (PDG de The Metals Company, voir plus haut) et Michael Lodge. Barron y déclarait sans ambages « *Nous voulons contribuer à la mise en place de cette législation très délicate [relative à l'exploitation minière], et je pense qu'il sera bénéfique pour nous tous de la tenir à l'écart de l'attention du public* ». Ce manque de transparence se traduit, notamment, par le fait que les États membres de l'AIFM n'ont pas accès à certaines informations capitales tel que le nom des entreprises qui ne communiquent pas les données environnementales nécessaires. Une situation qui a déjà fait l'objet de critiques de la part des organisations de défense de l'environnement, mais également de la part de certains États Parties tels que la Norvège et le Mexique[97].

d. Une catastrophe écologique annoncée

En 2018, GSR a dévoilé son nouveau robot collecteur de nodules polymétalliques – ces concrétions situées dans les fonds marins et potentiellement riches en métaux, voir plus haut –, le *Patania II* à Anvers. La présentation du robot à Anvers s'est faite en présence de deux cadres de l'entreprise et de Michael Lodge. Trois ans plus tard, GSR a mené une mission test au sein de la zone d'exploration que l'AIFM lui a concédée. Bien que l'entreprise vante une opération réussie, le test a rapidement démontré les limites et les risques relatifs au déploiement d'un monstre mécanique de douze mètres de long lourd de vingt-cinq tonnes dans les fonds marins. Et pour cause, le robot chargé de collecter les nodules et relié au bateau de GSR s'est accidentellement détaché de ce dernier. Celui-ci a du être récupéré par l'entreprise à plusieurs milliers de mètres de profondeur[98]. En parallèle, des militants de Greenpeace ont surveillé les opérations de GSR et inscrit « *Risk* » sur le bateau de l'entreprise afin d'alerter sur les risques pour l'environnement de l'extraction minière en eaux profondes[99]. Pourtant, malgré cet alarmant second test (un premier test technique préliminaire avait eu lieu en 2019 et s'était heurté à des dysfonctionnements techniques[100]), GSR estime qu'avec deux robots miniers, elle sera en mesure de collecter trois millions de nodules par an[101]. Et pour cause, les robots qui devraient être déployés en cas d'octroi de permis d'exploitation seraient quatre fois plus importants[102]. Dans tous les cas, collecter des nodules semble légèrement plus compliqué et dangereux qu'« aspirer une balle de golf »…

Les craintes relatives à l'impact sur l'environnement de l'exploitation minière en eaux profondes sont nombreuses tant dans

le chef des militants écologistes qu'au sein du monde académique. En ce sens, deux temporalités s'affrontent. D'une part, celle de l'industrie et de la géopolitique qui voient dans l'exploitation minière en eaux profondes, respectivement, de nouvelles parts de marché et une opportunité de diversifier l'approvisionnement en matières premières. Et d'autre part, celle de la recherche scientifique qui nécessite des examens approfondis sur le long terme afin d'évaluer avec précision les conséquences d'une telle entreprise dans un milieu si peu connu[103]. Michael Lodge, secrétaire général de l'AIFM déclarait, pour sa part, dans une interview accordée au magazine *The Economist* en décembre 2019 que les conséquences environnementales de l'exploitation minière en eaux profondes étaient « prévisibles et gérables »[104].

Certains dommages environnementaux seraient durables, voire irréversibles

Pourtant, les plaines abyssales dans lesquelles se trouvent les nodules constituent un habitat pour de nombreuses espèces sous-marines végétales et animales. Or, au vu de la complexité de mener des études à de telles profondeurs, il n'existe que peu de données sur la faune gravitant autour des nodules[105]. Néanmoins, certaines observations ont conclu à une présence plus importante de faune sessile[106] et mobile dans les zones riches en nodules[107]. Dans le même temps, un consortium de chercheurs qui accompagnait la mission de GSR a répertorié de nombreux dégâts environnementaux liés à la collecte des nodules. L'opération aurait généré un déplacement de sédiments sur cinq cents mètres de part et d'autre de la zone exploitée.

Dans le même temps, six cent soixante-deux scientifiques ont signé une pétition pointant le manque de connaissances relatives aux impacts environnementaux de l'exploitation minière en eaux profondes pour pouvoir rédiger une législation appropriée[108].

Le manque de recul temporel par rapport aux premiers tests d'exploitation minières en eaux profondes effectués ne permet pas d'observer si, et à partir de combien de temps après la fin de l'exploitation, le milieu pourrait se rétablir. Les traces laissées des décennies plus tard par un test d'extraction minière mené dans la zone de Clarion Clipperton en 1978 laissent néanmoins penser que certains dommages environnementaux seraient durables, voire irréversibles. Et pour cause, à ces profondeurs, le peu de lumière, d'énergie et de nourriture disponibles rendent les processus de régénération extrêmement lents. Par ailleurs, l'exploitation minière en eaux profondes pourrait altérer le stockage océanique de CO_2. En d'autres termes, l'exploitation minière en eaux profondes pourrait renforcer la dynamique de réchauffement climatique. Dans ce cadre, justifier l'exploitation minière en eaux profondes comme un moyen de lutter contre le réchauffement climatique apparaît, pour le moins, paradoxal.

Conclusion

La « double transition » a été présentée par l'Union européenne dans le Pacte vert pour l'Europe comme un état de fait, un objectif politique vers lequel il convient de tendre par le biais de règlements et de directives. La question, pourtant fondamentale, « avons-nous les moyens de nos ambitions ? », semble pour sa part avoir été reléguée au second plan. Néanmoins, la réponse à cette question est loin de couler de source. Tout d'abord, d'un point de vue physique et technique. Puisque, nous l'avons vu, en l'état, l'offre de certains métaux stratégiques ne sera pas en mesure de suivre la croissance de la demande. En effet, les impératifs techniques et logistiques que nécessitent le développement de nouvelles mines s'opposent aux échéances visées par les autorités européennes. Ensuite, les conséquences environnementales et climatiques d'un développement aussi important de l'industrie extractive s'opposent aux objectifs qui la justifient à savoir, la lutte contre le réchauffement climatique et la préservation des ressources. Dans le même temps, nous l'avons vu avec Walzinc, l'impact environnemental de l'exploitation minière génère de vives tensions dans le chef des populations concernées par de nouveaux projets, en particulier, dans le cadre d'une relance du secteur en Europe.

Toutes ces limites ont mené l'industrie à se pencher sur de nouvelles sources d'approvisionnement dont l'exploitation minière en eaux profondes. Les risques climatiques et environnementaux relatifs à une telle exploitation apparaissent en contradiction complète avec le discours de ses promoteurs qui promettent « une solution simple au problème du réchauffement climatique ». En réalité, la polémique relative à l'exploitation minière en eaux profondes révèle le paradoxe fondamental qui sous-tend la stratégie à long terme de l'UE. En effet, dès sa présentation, le Pacte vert pour l'Europe a été défini en tant que « stratégie de croissance ». Trois ans après la publication de cette stratégie par la Commission européenne, ce paradoxe apparaît de plus en plus visible. En ce sens, les institutions européennes et les États membres seront tôt ou tard obligés de trancher. Le Pacte vert et la « double transition » constituent-ils un véritable engagement politique visant à faire baisser les émissions de gaz à effet de serre ou un simple narratif autour d'un plan de relance de la production et la consommation intérieures ? Une chose est, cependant, certaine. Une croissance de la demande en matières premières poussée par la démultiplication d'objets à la valeur d'usage plus que douteuse (aspirateurs connectés, frigos intelligents et autres « smart » brosses à dents…) constitue un non-sens écologique et

physique. À la lumière de cette analyse, il semble que seule une planification écologique basée sur une démocratisation des choix de production (Pourquoi extrait-on ce métal ? Qu'est ce que cela implique d'un point de vue environnemental et climatique ?) puisse encadrer raisonnablement l'exploitation des matières premières. Laissé au bon vouloir du marché, la « double transition » pourrait bien se solder par un saccage du patrimoine mondial de l'humanité.

[1] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Le pacte vert pour l'Europe, Bruxelles : Commission européenne, 11 décembre 2019, COM(2019) 640 final. Proposition de règlement du Parlement et du Conseil établissant un cadre visant à garantir un approvisionnement sûr et durable en matières premières critiques et modifiant les règlements (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1724 et (UE) 2019/1020, Bruxelles : Commission européenne, 16 mars 2023, COM(2023) 160 final.

[2] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Un approvisionnement sûr et durable en matières critiques à l'appui de la double transition, Bruxelles : Commission européenne, 16 mars 2023, COM(2023) 165 final.

[3] Un minerai est une roche constituée de minéraux. Un minéral pour sa part désigne une susbtance chimique cristalline et généralement inorganique. Certains minéraux contiennent des éléments métalliques tels que les métaux dont il est question dans cette analyse.

[4] Carolan J., « Digital Devices Took Over Our Lives in 2020 : Here's How to Stay Secure », Forbes.com, 15 avril 2021, [en ligne :] https://www.forbes.com/sites/forbestechcouncil/2021/04/15/digital-devices-took-over-our-lives-in-2020-heres-how-to-stay-secure/?sh=189728d1ed27, consulté le 18 avril 2023.

[5] Balbi G. *et al.*, « Digital Circulation: Media, Materiality, Infrastructures. An Introduction », Tecnoscienza, 2016, vol. VII, n°1, 14 p., [en ligne :] http://www.tecnoscienza.net/index.php/tsj/article/view/250, consulté le 12 juin 2023. Voir également : Dejong M., « Et si on faisait le poing sur l'obsolescence programmée ? », Bruxelles : CPCP, Analyse n° 423, 2020, [en ligne :] http://www.cpcp.be/publications/poing-obsolescence, consulté le 12 juin 2023.

[6] Le Page M., « Streaming online pornography produces as much CO2 as Belgium », Newscientist.com, 11 juillet 2019, [en ligne :] https://www.newscientist.com/article/2209569-streaming-online-pornography-produces-as-much-co2-as-belgium, consulté le 11 mai 2023.

[7] Taffel S., « Data and oil metaphor : materiality and metabolic rifts », New Media & Society, 2021, vol. XXV, n°5, p. 1-19. Voir également Lejeune R., « Cryptomonnaies, NFT et blockchains. Entre influence et désillusions », Bruxelles : CPCP, analyse n°481, 2023, [en ligne :] https://www.cpcp.be/publications/cryptomonnaies/.

[8] Ferreboeuf *et al.*, *op. cit.*

[9] Le paradigme cornucopien repose sur la croyance que les innovations technologiques vont permettre à la société de répondre à ses besoins sans entrave.

[10] Pervasif signfie que les données « se diffusent à travers toutes les parties du systèmes d'informations » (lalanguefrancaise.com). En d'autres termes, cela signifie que les services et les terminaux interagissent entre eux ce qui permet d'être connecté aux réseaux de façon permanente.

[11] Vidal O., « Ressources minérales, progrès technologique et croissance », Approches temporelles du développement durable, 2018, n°28, [en ligne :] https://journals.openedition.org/temporalites/5677?lang=en.

[12] Numérique fr

[13] Taffel S., « Data and oil : metaphor, materiality and metabolic rifts », New Media & Society, 2021, [en ligne :] https://journals.sagepub.com/doi/10.1177/14614448211017887, consulté le 18 avril 2023.

[14] « Numérique responsable : et si nous adoptions les bons réflexes ?», Dossier Presse, Paris : Ademe, 19 janvier 2022, [en ligne :] https://presse.ademe.fr/wp-content/uploads/2022/01/DP_Numerique-responsable-190122.pdf

[15] Directrice de « projets technologiques et solutions numériques émergentes » au sein de la Direction générale des Entreprises de l'État français d'octobre 2020 à novembre 2021.

[16] Dedryver L. avec l'aide de Couric V., « La consommation des métaux du numérique : un secteur loin d'être dématérialisé », France Stratégie, Document de travail, juin 2020, n°2020-05, [en ligne :] https://www.strategie.gouv.fr/publications/consommation-de-metaux-numerique-un-secteur-loin-detre-dematerialise, consulté le 18 avril 2023.

[17] « Tellure », Lelementarium.fr, s.d., [en ligne :] https://lelementarium.fr/element-fiche/tellure, consulté le 10 mai 2023.

[18] « Cobalt », Lelementarium.fr, s.d., [en ligne :] https://lelementarium.fr/element-fiche/cobalt, consulté le 13 juin 2023.

[19] Digital Economy Growth and Mineral Resources. Implications for Developing Countries. UNCTAD Technical Notes on ICT for Development, Genève : Conférence des Nations unies sur le commerce et le développement, n°16, decembre 2020, p.9.

[20] Dedryver L., *op. cit.*

[21] Entretien Thinkerview du 25 janvier 2022. Sources et compléments, Paris : Systex, 58 p.

[22] Conférence des Nations Unies sur le commerce et le développement, *op. cit.*

[23] *Ibid.*

[24] « Indium », Lelementarium.fr, s.d., [en ligne :] https://lelementarium.fr/element-fiche/indium, consulté le 11 mai 2023. Voir également le site web d'Umicore : www.umicore.be/fr/our-sites/hoboken/, consulté le 15 mai 2023.

[25] Geldron A., L'épuisement des métaux et minéraux : faut-il s'inquiéter ?, Paris : Ademe, juin 2017, 23 p., [en ligne :] https://www.researchgate.net/publication/323119968_L%27EPUISEMENT_DES_METAUX_ET_MINERAUX_FAUT-IL_S%27INQUIETER_L%27EPUISEMENT_DES_METAUX_ET_MINERAUX_FAUT-IL_S%27INQUIETER, consulté le 12 juin 2023.

[26] Vidal O., *op. cit.*, voir également : de Guillebon B., « Quel futur pour les métaux ? », *Géologues*, 2012, n°170, p. 23-25, [en ligne :] https://www.geosoc.fr/metiers-formations/domaines-d-activites/ressources-minerales/pour-en-savoir-plus/tensions-et-contraintes-des-substances-minerales/352-quel-futur-pour-les-metaux/file.html, consulté le 15 mai 2023.

[27] SystExt, 2022, *op. cit.*, p. 8.

[28] Il est cependant possible que, dans le futur, on découvre et exploite de nouveaux gisements qui présenteraient de plus fortes teneurs en métal, notamment, à des profondeurs plus importantes.

[29] Lacs salés asséchés totalement ou en partie situés dans la Cordillère des Andes.

[30] Controverses minières. Pour en finir avec certaines contrevérités sur la mine et les filières minérales, Vol. I, SystExt, 16 septembre 2021, 162 p., [en ligne :] https://www.systext.org/node/1785, consulté le 18 avril 2023.

[31] Geldron A., *op. cit.*, voir par exemple : Harmsen J., Roes A.et Patel M., « The impact of copper scarcity on efficiency of 2050 global renewable scenarios », Energy, février 2013, vol. L, n° 1, [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S0360544212009139, consulté le 18 avril 2023.

[32] L'Accord vise notamment à « poursuivre les efforts » afin de limiter le réchauffement de la température moyenne mondiale à 1,5°par rapport à l'ère préindustrielle.

[33] The Role of Critical Minerals in Clean Energy Transitions, Paris : Agence internationale de l'énergie, mai 2021, 283 p., [en ligne :] https://www.iea.org/reports/the-role-of-critical-minerals-in-clean-energy-transitions, consulté le 11 mai 2023.

[34] Dedryver L., *op. cit.*

[35] « Boucles du Hainaut : les orientations du projet validées par la Wallonie », Wallonie.be, 18 novembe 2020, [en ligne :] https://www.wallonie.be/fr/actualites/boucle-du-hainaut-bilan-de-la-consultation-citoyenne, consulté le 20 avril 2023.

[36] « La boucle du Hainaut : un dossier électrique sous haute tension qui agite bourgmestres et riverains dans le Hainaut », Rtbf.be, 15 février 2023, [en ligne :] https://www.rtbf.be/article/la-boucle-du-hainaut-un-dossier-electrique-sous-haute-tension-qui-agite-bourgmestres-et-riverains-dans-le-hainaut-11152830, consulté le 20 avril 2023.

[37] Règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/631 en ce qui concerne le renforcement des normes de performance en matière d'émissions de CO2 pour les voitures particulières neuves et les véhicules utilitaires légers neufs conformément à l'ambition accrue de l'Union en matière de climat, Bruxelles : Commission européenne, 14 juillet 2021, COM(2021) 556 final, [en ligne :] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021PC0556, consulté le 20 avril 2023.

[38] Agence internationale de l'énergie, *op. cit.*

[39] Dedryver L., *op. cit.*

[40] Voir : COM(2023) 165 final, op. cit

[41] Proposition de règlement du Parlement et du Conseil établissant un cadre visant à garantir un approvisionnement sûr et durable en matières premières critiques et modifiant les règlements (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1724 et (UE) 2019/1020, Bruxelles : Commission européenne, 16 mars 2023, COM(2023) 160 final.

[42] « Lauch of the Route 35 Platform. Our priorities for achieving our electrification goals. Speech by Commissioner Thierry Breton », Ec.europa.eu, 15 décembre 2022, [en ligne :] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_7785, consulté le 20 avril 2023.

[43] « Charted: The rise of battery-only electric cars in the EU », Weforum.org, 1er mars 2023, [en ligne :] https://www.weforum.org/agenda/2023/03/battery-only-electric-passenger-cars-eu, consulté le 10 mai 2023.
Notons, par ailleurs, que sous la pression de l'Allemagne, la Commission européenne a infléchi sa position, ouvrant la porte aux véhicules roulant avec des carburants de synthèse par de-là 2035.

[44] COM(2023) 160 final, *op. cit.*

[45] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Un approvisionnement sûr et durable en matières critiques à l'appui de la double transition, Bruxelles : Commission européenne, 16 mars 2023, COM(2023) 165 final.
Pour un résumé, voir : « Matières premières critiques: garantir des chaînes d'approvisionnement sûres et durables pour l'avenir écologique et numérique de l'UE », Ec.europa.eu, 16 mars 2023, [en ligne :] https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_1661, consulté le 11 mar 2023.

[46] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Le pacte vert pour l'Europe, Bruxelles : Commission européenne, 11 décembre 2019, COM(2019) 640 final.

[47] Peers C., « Note on the Critical Raw Materials Act », Teneo.com, 30 mars 2023, [en ligne :] https://www.teneo.com/note-on-the-critical-raw-materials-act, consulté le 11 mai 2023.

[48] COM(2023) 160 final, p. 7, *op. cit.*

[49] COM(2023) 165 final, *op. cit.*

[50] Peers C., *op. cit.*

[51] Dendooven L., « Des mines de lithium, gallium, germanium, vont-elles s'ouvrir en Belgique et en Europe pour diminuer notre dépendance à la Chine ? », Rtbf.be, 26 juillet 2022, [en ligne :] https://www.rtbf.be/article/des-mines-de-lithium-gallium-germanium-vont-elles-souvrir-en-belgique-et-en-europe-pour-diminuer-notre-dependance-a-la-chine-11032847, consulté le 3 mai 2023.

[52] Xavier-Lefèvre F., « La Wallonie dépoussière son code minier et sauvegarde ses terrils », Lecho.be, 12 décembre 2018, [en ligne :] https://www.lecho.be/economie-politique/belgique/wallonie/la-wallonie-de-poussiere-son-code-minier-et-sauvegarde-ses-terrils/10078231.html, consulté le 3 mai 2023.

[53] Ferreboeuf *et al.*, *op. cit.*

[54] Witchalls S., « The Environmental Problems caused by mining », Earth.org, 3 avril 2022, [en ligne :] https://earth.org/environmental-problems-caused-by-mining, consulté le 11 mai 2023.

[55] « Climate Risk and decarbonisation: What every mining CEO needs to know », Mckinsey.com, 28 janvier 2020, [en ligne :] https://www.mckinsey.com/capabilities/sustainability/our-insights/climate-risk-and-decarbonization-what-every-mining-ceo-needs-to-know, consulté le 13 juin 2023

[56] Agence internationale de l'énergie, *op. cit.*

[57] Mononen T. *et al.*, « Social and environmental impacts of mining activities in the EU », Bruxelles : Parlement européen, étude commandée par la Commission PETI, mai 2022, 80 p., [en ligne :] https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)729156, consulté le 11 mai 2023.

[58] Guerrero F. *et al.*, « Spain's greatest and most recent mine disaster », Disasters, 2008, vol. XXXII, n°1, p. 19-40, [en ligne :] https://pubmed.ncbi.nlm.nih.gov/18217916, consulté le 10 mai 2023.

[59] Kovac C., « Cynaide spill could have long term impact », British Medical Journal, mai 2000, vol. CCCXX, [en ligne :] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1127303, consulté le 10 mai 2023.

[60] Tran M., « Hungary toxic sludge spill an 'ecological catastrophe' says governement », Theguardian.com, 5 octobre 2010, [en ligne :] https://www.theguardian.com/world/2010/oct/05/hungary-toxic-sludge-spill, consulté le 10 mai 2023.

[61] SystExt, *op. cit.*

[62] « What is the Environmental Impact of the Mining Industry ? », Worldatlas.com, 25 avril 2017, [en ligne :] https://www.worldatlas.com/articles/what-is-the-environmental-impact-of-the-mining-industry.html, consulté le 11 mai 2023.
SystExt, *op. cit.*

[63] Huffy M., « Abandoned Mines: The Scars of the Past », Global Challenges, novembre 2019, n°6, [en ligne :] https://globalchallenges.ch/issue/6/abandoned-mines-the-scars-of-the-past.

[64] Worlanyo A. S. et Jiangfeng L., « Evaluating the environmental and economic impact of mining for post-mined land restoration and land-use: A review », Journal of Environmental Management, 2021 vol. CCLXXIX, 111623.

[65] Mononen *et al.*, *op. cit*

Taffel S., *op. cit.*

[66] Leterme C., « L'angle mort écologique de la course aux semi-conducteurs », Gresea.be, 6 avril 2023, [en ligne :] https://gresea.be/L-angle-mort-ecologique-de-la-course-aux-semi-conducteurs, consulté le 10 mai 2023.

[67] « Les nodules », Geo-ocean.fr, dernière modification le 21 décembre 2017, [en ligne :] https://www.geo-ocean.fr/Science-pour-tous/Nos-salles-d-etudes/Les-ressources-minerales-non-energetiques/Les-nodules, consulté le 04 mai 2023.

[68] « Encroûtements cobaltifères », Geo-ocean.fr, dernière modification le 25 mars 2022 , [en ligne :] https://www.geo-ocean.fr/Expertise/Appui-a-la-Puissance-Publique/Les-ressources-minerales-grand-fond/Encroutements-cobaltiferes, consulté le 04 mai 2023.

[69] « Sulfures polymétalliques hydrothermaux », Geo-ocean.fr, dernière modification le 25 août 2017, [en ligne :] https://www.geo-ocean.fr/Expertise/Appui-a-la-Puissance-Publique/Les-ressources-minerales-grand-fond/Sulfures, consulté le 04 mai 2023.

[70] Pour en savoir plus sur Gerard Barron et son parcours dans le secteur de l'exploitation minière en eaux profondes : Schek J., B. Eliot et Foldy B., « Environemental Investing Frenzy Streches Meaning of 'Green' », Wsj.com, 24 juin 2021, [en ligne :] https://www.wsj.com/articles/environmental-investing-frenzy-stretches-meaning-of-green-11624554045, consulté le 11 mai 2023.

[71] Baker A., « A Climate Solution Lies Deep Under the Ocean – But Accessing It Could Have Huge Environmental Costs », Time.com, 7 septembre 2021, [en ligne :] https://time.com/6094560/deep-sea-mining-environmental-costs-benefits/, consulté le 11 mai 2023.

[72] Le siège social de la maison mère, DEME, se situe à Zwijndrecht en Province d'Anvers. DEME est détenu par le holding Ackermans & Van Haaren (AVH). Alexia Bertrand, la fille de Luc Bertrand, président du holding, est secrétaire d'État au Budget et à la Protection des consommateurs, adjointe au ministre de la Justice et de la mer du Nord. Elle était auparavant la cheffe de cabinet de Didier Reynders, alors ministre des Affaires étrangères (2015-2019).

[73] Baker A., *op. cit.*

[74] Kaikkonen L. et Virtanen E., « Shallow-water mining undermines global sustainability goals », Trends in Ecology & Evolution, novembre 2022, vol. XXXVII, n°11, p. 931-934, [en ligne :] https://www.sciencedirect.com/science/article/pii/S0169534722001963, consulté 8 mai 2023.

[75] Pim J. *et al.*, At a crossroads : Europe's role in deep-sea mining, Bruxelles : Seas at Risk, 2021, 88 p., [en ligne :] https://seas-at-risk.org/wp-content/uploads/2021/05/At-a-Crossroads-Europes-role-in-Deep-sea-mining.pdf, consulté le 8 mai 2023.

[76] Convention des Nations unies sur le droit de la mer, Montego Bay : Nations Unies, 10 décembre 1982, [en ligne :] https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&clang=_fr, consulté le 15 mai 2023.

[77] https://www.nature.com/articles/s41893-020-0558-x?proof=t.

[78] Baker A., *op. cit.*

[79] Willaert K., Assessment of the Belgian Legislation on Deep Sea Mining, Bruxelles : WWF et Maritime Institute, avril 2019, 9 p.

[80] « Loi relative à la prospection, l'exploration et l'exploitation des ressources des fonds marins et leur sous-sol au-delà des limites de la juridiction nationale », Le Moniteur belge, 16 septembre 2013, p. 65612 et « Arrêté royal concernant la prospection, l'exploration et l'exploitation des ressources des fonds marins et leur sous-sol au-delà des limites de la juridiction nationale », Le Moniteur belge, 15 octobre 2013, p. 73061.

[81] Willaert K., *op. cit.*

[82] Singh P., « What Are the Next Steps for the International Seabed Authority after the Invocation of the 'Two-year Rule'? », The International Journal of Marine and Coastal Law, 2021, vol. XXXVII, n°1, p. 152-165, [en ligne:] https://brill.com/view/journals/estu/37/1/article-p152_7.xml?language=en, consulté le 15 mai 2023.

[83] Projet de règlement relatif à l'exploitation des ressources minérales dans la Zone, Kingston : Autorité internationale des fonds marins, 22 mars 2019, ISBA/25/C/WP.1, [en ligne :] https://www.isa.org.jm/wp-content/uploads/2022/06/isba_25_c_wp1-f_0.pdf, consulté le 15 mai 2023.

McKie R., « Deep-sea mining for rare metals will destroy ecosystems, say scientists », Theguardian.com, 26 mars 2023, [en ligne :] https://www.theguardian.com/environment/2023/mar/26/deep-sea-mining-for-rare-metals-will-destroy-ecosystems-say-scientists, consulté le 15 mai 2023.

[84] « Belgium helps decide on the seabed's fate – 11 Questions », Diplomatie.belgium.be, 30 mars 2023, [en ligne :] https://diplomatie.belgium.be/en/policy/policy-areas/highlighted/belgium-helps-decide-seabeds-fate-11-questions, consulté le 15 mai 2023.

[85] Pour consulter le communiqué de presse : https://www.dosi-project.org/wp-content/uploads/DOSI_ISA_Nauru.pdf, Baker A., *op. cit.*

[86] « La Belgique doit rejoindre l'alliance des pays pour un moratoire sur l'exploitation minière des fonds marins », Lesoir.be, 9 mars 2023, [en ligne :] https://www.lesoir.be/499823/article/2023-03-09/la-belgique-doit-rejoindre-lalliance-des-pays-pour-un-moratoire-sur, consulté le 15 mai 2023.

[87] Diplomatie.belgium.be, *op. cit.*

[88] *Ibid.*

[89] « Following Palau's Leadership, FSM to join Alliance of Countries for Deep-sea Mining Moratorium; President Panuelo to Solicit Members

of Pacific Islands Forum to Oppose Deep-sea Mining », Gov.fm, 10 juillet 2022, [en ligne :] https://gov.fm/index.php/component/content/article/27-fsm-pio/news-and-updates/622-following-palaus-leadership-fsm-to-join-alliance-of-countries-for-a-deep-sea-mining-moratorium-president-panuelo-to-solicit-members-of-pacific-islands-forum-to-oppose-deep-sea-mining?Itemid=177, consulté le 15 mai 2023.

[90] Limb L., « France votes to ban deep-sea mining in its waters: Why is this practice so controversial? », Euronews.com, 22 janvier 2023, [en ligne :] https://www.euronews.com/green/2023/01/18/france-votes-to-ban-deep-sea-mining-in-its-waters-why-is-this-practice-so-controversial, consulté le 9 mai 2023.

[91] Résolution du Parlement européen du 9 juin 2021 sur la stratégie de l'UE en faveur de la biodiversité à l'horizon 20230 : Ramener la nature dans nos vies, Strasbourg : Parlement européen, 9 juin 2021, A9-0179/2021, [en ligne :] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0277_EN.html, consulté le 15 mai 2023.

[92] « Global Parliamentary Declaration Calling for a Moratorium on Deep Seabed Mining », Pgaction.org, s.d., [en ligne :] https://www.pgaction.org/ilhr/oceans/call-for-moratorium-on-deep-seabed-mining.html, consulté le 15 mai 2023.

[93] Willaert K., « The Entreprise: State of Affairs, challenges and Way Forward », Marine Policy, 2021, vol. CXXXI, 104590, [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S0308597X21002013, consulté le 15 mai 2023.

[94] Woody T. et Halper E., « A gold rush in the deep sea raises questions about the authority charged with protecting it », Latimes.com, 19 avril 2022, [en ligne :] https://www.latimes.com/politics/story/2022-04-19/gold-rush-in-the-deep-sea-raises-questions-about-international-seabed-authority, consulté le 15 mai 2023.

[95] « Assembly Elects Michael Lodge of the United Kingdom as Next Secretary-General of Seabed Authority; Hears Address by Prime Minister of Trinidad and Tobago », Isa.org, 22 juillet 2016, [en ligne :] https://www.isa.org.jm/news/assembly-elects-michael-lodge-united-kingdom-next-secretary-general-seabed-authority-hears, consulté le 15 mai 2023.

[96] Woody T. et Halper E., *op. cit.*

[97] McKie R.,*op. cit.*

[98] « Deep sea mining tests resume after robot rescued from Pacific Ocean floor », Reuters.com, 1er mai 2021, [en ligne :] https://www.reuters.com/business/environment/deep-sea-mining-tests-resume-after-robot-rescued-pacific-ocean-floor-2021-04-30, consulté le 8 mai 2023.

[99] « Nouvelles actions contre l'exploitation minière des grands fonds marins ! », Greenpeace.org, 22 avril 2021, [en ligne :] https://www.greenpeace.org/belgium/fr/blog/21708/nouvelles-actions-contre-lexploitation-miniere-des-grands-fonds-marins, consulté le 8 mai 2023.

[100] Custers R., « La Belgique en eaux profondes. Comment la Belgique s'est muée en un redoutable acteur des grands fonds marins », Gresea.be, 17 juillet 2020, [en ligne :] https://gresea.be/La-Belgique-en-eaux-profondes-Comment-la-Belgique-s-est-muee-en-un-redoutable#nb7, consulté le 8 mai 2023.

[101] Baker A., *op. cit.*

[102] Weiss S., « La menace écologique de l'exploitation minière en eaux profondes », Nationalgeographic.fr, 5 avril 2022, [en ligne :] https://www.nationalgeographic.fr/environnement/la-menace-ecologique-de-lexploitation-miniere-en-eaux-profondes, consulté le 8 mai 2023.

[103] Hannington M., Peterson S. et Krätschell A., « Subsea mining moves closer to shore », Nature Geoscience, 2017, vol. X, p. 158-159, [en ligne :] https://www.nature.com/articles/ngeo2897, consulté le 15 mai 2023.

[104] https://ocean.economist.com/innovation/articles/is-deep-sea-mining-part-of-the-blue-economy.

[105] Tilot V., Biodiversité et distribution de la mégafaune. Vol. 1: Ecosystème de nodules polymétalliques de l'océan Pacifique Est équatorial ; Vol. 2 : Atlas photographique annoté des échinodermes de la zone de fractures de Clarion et de Clipperton, Paris : UNESCO/IOC, 2006, 62 p.

[106] Il s'agit des animaux vivant fixés à un susbstrat.

[107] Miller K. *et al.*, « An Overview of Seabed Mining Including the Current State of Development, Environmental Impacts, and Knowledge Gaps », Frontiers in Marine Science, 2018, vol. IV, n°418, [en ligne :] https://www.frontiersin.org/articles/10.3389/fmars.2017.00418/full, consulté le 15 mai 2023.

[108] Woody T. et Halper E., *op. cit.*

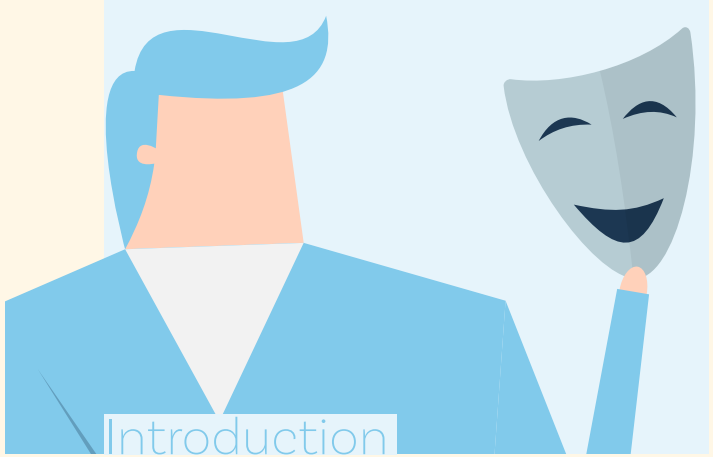
Philippe Courteille est licencié en journalisme et communication de l'ULB. Il a travaillé comme journaliste-réalisateur freelance pour de nombreuses émissions de télévision pendant 25 ans. Il est aujourd'hui responsable de la thématique Médias & Actions citoyennes chez Citoyenneté & Participation.

Deepfakes

Le mensonge à l'ère de l'intelligence artifcielle

Philippe Courteille

Étude



Introduction

« Mentez, mentez, il en restera toujours quelque chose ». Cette célèbre, et peut-être apocryphe, citation de Voltaire n'est malheureusement pas dénuée de vérité. Le souci est que les quelques rumeurs que partageaient nos aïeux en petit comité se sont transformées, depuis Internet et les réseaux sociaux, en flots continus et mondialement diffusés des fameuses fake news, ou désinformations intentionnelles, qui furent l'objet de notre dernière étude[1]. Celles-ci sont particulièrement rentables car plus partagées sur les réseaux que les informations avérées[2]. Elles peuvent aller des plus légères aux plus déstabilisantes, des plus basiques aux plus élaborées comme désormais les deepfakes ou *hypertrucages*. Ringards les textes pernicieux bien ficelés ou les trucages photos staliniens, désormais, les logiciels offrent la possibilité d'imiter l'écriture[3] et la voix de n'importe qui, tout comme de changer le mouvement des lèvres, le visage ou le corps d'une personnalité sur une vidéo pour lui faire dire et/ou faire ce qu'elle n'a jamais dit et/ou fait. Et l'intelligence artificielle accélère leur perfectionnement. Déjà des sites proposent d'en réaliser en quelques minutes. Ces technologies, qui évoluent à une vitesse vertigineuse, sont désormais à la portée de tout individu, mais aussi de toute équipe de communication ou de dirigeants malintentionnés.

Glenn Kessler, le rédacteur en chef de la chronique de vérification des faits du *Washington Post*, soulignait déjà en 2019 : « *Nous avons vu une explosion de vidéos qui sont délibérément déformées, ou qui sont en train d'être montées d'une manière ou d'une autre pour changer la façon dont les gens voient ce qui s'est passé, cela va jusqu'aux deepfakes (…) Au cours des deux dernières années, nous avons étendu le factchecking*[4] *aux vérifications de faits vidéo. Ils obtiennent cinq fois plus de vues que nos vérifications des faits de texte. C'est une indication du nombre de personnes supplémentaires qui obtiennent leurs informations par vidéo plutôt que par écrit* »[5].

Depuis, les spéculations vont bon train quant aux dérives hypothétiques d'un tel outil mis entre les mains du premier venu. Cela flirte parfois avec la science-fiction mais nous allons tenter d'énumérer les plus vraisemblables et d'en analyser les risques potentiels.

Mentez, mentez, il en restera toujours quelque chose

L'un des premiers deepfakes européens a eu lieu en Belgique dès 2019 et même la Première ministre Sophie Wilmes en a été victime l'année suivante, sans conséquence sur la crédibilité de celle-ci. Mais en 2023 un rapport de la société Sumsub[6], entreprise anglaise de sécurité en ligne, annonce que la Belgique fait partie des pays les plus touchés par l'explosion des deepfakes voyant le nombre de fraudes par deepfake exploser de 2 950 % cette année-là, presque autant que les Américains, avec +3 000 % de cas[7].

Le sujet était relativement peu abordé en Europe avant 2022-23, en comparaison avec les craintes qu'il suscite aux États-Unis depuis cinq, six ans. Il faut dire que ce pays est encore sous le coup des élections de 2016 et du scandale Cambridge Analytica ou encore des immixtions russes dans ce processus électoral. Depuis l'élection de Donald Trump et le Brexit, les fake news cumulées aux données personnelles des citoyens sont vues comme une arme de propagande très tentante pour des équipes politiques à travers le monde. Beaucoup d'élites américaines se demandent quelles seraient dès lors les conséquences de vidéos truquées dans les campagnes à venir, d'autant que les dernières étaient de plus en plus nauséabondes. Rappelons que Donald Trump n'hésitait pas à déclarer qu'Obama n'était pas américain, à qualifier Hillary Clinton de « crooked »[8], « crapule » en français, Joe Biden de « sleeping Joe », Joe l'endormi, et Kamala Harris de « folle », de « stupide comme un roc » et de « clocharde ». Dès 2019, Trump était capable de partager à chaud sur Twitter des photos et des vidéos de désinformations, notamment à l'encontre de Nancy Pelosi, présidente démocrate de la Chambre des représentants. Mais l'usage des hypertrucages était resté anecdotique en politique jusqu'en 2024, année qui a vu leur multiplication et des élections pour la moitié de l'Humanité. D'autant que Trump est désormais soutenu par Elon Musk, un homme influent et peu regardant sur la véracité des informations qui circulent sur son réseau X (ex Twitter), tout comme sur l'utilisation de son IA Grok pour propager de la désinformation et des deepfakes. Le camp démocrate ne manque pas non plus de mordant et est capable, dans sa communication, de flirter avec les limites de la bienséance voire de la légalité.

Désormais ces trucages deviennent bluffant et se multiplient dans nombres de propagandes, d'arnaques ou d'intimidations. Et nous le verrons, les femmes en subissent de particulièrement perverses et violentes.

Internet est devenu l'empire de la désinformation et beaucoup de responsables et de spécialistes s'en inquiètent, allant jusqu'à parler « l'infocalypse »[9] . Mais est-il vraiment raisonnable d'imaginer

qu'un jour une majorité de citoyens, excités par la lumière bleue de leurs écrans, espérant y trouver la lune tels des papillons de nuit devant une ampoule incandescente, prendraient le risque d'y brûler les ailes de leur liberté démocratique ? Rien n'est moins sûr, même si pour beaucoup mieux vaut prévenir que guérir.

En revanche, ce qui est clair, c'est que le terrain numérique, source de débats polarisés et de croissance des partis extrémistes, est de plus en plus propice à une désinformation par l'image et/ou le son, avec un réalisme déconcertant. Le tout propagé à grande vitesse par des bots, des robots, chargés de les disséminer par millions. « *Un mensonge répété dix fois reste un mensonge, répété mille fois, il devient alors une vérité* », cette phrase attribuée à Joseph Goebbels, l'un des plus implacables propagandistes de l'Histoire, résume assez bien une méthode qui a fait ses preuves.

Nous tentons dans cette publication d'évaluer les risques qui peuvent en découler et les facteurs pouvant favoriser leur croissance, que ce soit au niveau sociétal, économique ou politique. Car si cet outil peut offrir une part d'amusement ou de sensibilisation, on constate d'ores et déjà qu'il perfectionne principalement la tromperie, la fraude, la vilenie et le chantage.

À l'aune des inquiétudes d'experts de la question, nous analysons ensuite les pistes de solutions.

Mais commençons par comprendre ce que sont les deepfakes et quelle est leur origine.

1. Deepfake, le profondément trompeur

Comme Saint Thomas, beaucoup ne croient que ce que qu'ils voient. Et dans notre monde de l'image toute puissante, les deepfakes risquent d'en déstabiliser plus d'un. Le terme est un mélange de *fake news*, soit une désinformation intentionnelle, et de *deep learning*, qui désigne un type d'intelligence artificielle où la machine « apprend » par elle-même, à partir de sa propre observation de divers phénomènes. On appelle ces derniers des algorithmes d'apprentissage, par opposition aux algorithmes de programmation qui se contentent d'exécuter des ordres donnés. « *Ce sont des faux, quelle que soit la nature du contenu - vidéo, photo, audio ou texte - conçus grâce à l'intelligence artificielle (…) Pour l'heure, les deepfakes les plus couramment diffusés sur internet sont des vidéos truquées dans lesquelles le visage et la voix d'une personne connue sont falsifiés, lui faisant dire ou faire ce qu'elle n'a jamais dit ou jamais fait* »[10]. Attention il s'agit bien d'un hypertrucage et non d'une astuce de montage, de type ralenti ou coupure d'une partie du discours, que beaucoup ont tendance à englober dans le terme deepfake et que d'autres nomment *cheapfake* (littéralement « le faux bon marché »). Par exemple si on coupe une partie du discours d'un homme politique pour lui faire dire autre chose.

Les deux algorithmes entretiennent une relation gagnant-gagnant

On savait que les hypertrucages vidéos étaient possibles après avoir vu au cinéma Forrest Gump serrer la main de JFK ou lorsque, dans le film *Rogue One, une histoire de Star Wars*, sorti en 2016, avec le personnage de Grand Moff, réapparu sous les traits de Peter Cushing, l'acteur qui l'avait incarné dans un épisode précédent de la saga et mort… en 1994, soit vingt-deux ans auparavant. Tout cela était fait par des studios professionnels avec d'énormes puissances de calcul pour modifier chaque image d'une vidéo. Ça demandait aussi de gros investissements ce qui limitait leur nombre et leur impact. Mais ça, c'était avant.

a. GAN, un ping-pong cognitif

Les évolutions technologiques, susceptibles de faire évoluer les deepfakes, explosent depuis quelques années et ne cessent de surprendre par leur réalisme grandissant. Ces progrès ont pu être réalisés, à la base, grâce à une technique appelée GAN (Generative Adversarial Networks) soit des Réseaux Antagonistes Génératifs en français. Il s'agit en fait d'une classe d'algorithmes d'apprentissages non supervisés par l'homme. En clair, deux réseaux sont placés en compétition. Le premier réseau est le « générateur », il génère par exemple une image, tandis que son adversaire, le « discriminateur » essaie de détecter si l'image est réelle, à partir de sa base de données d'images, ou bien si elle est le résultat du générateur. Ces deux réseaux s'entraînent l'un l'autre dans le cadre d'une relation contradictoire, s'échangeant les données et les résultats de leurs analyses. Les deux algorithmes entretiennent donc une relation gagnant-gagnant d'amélioration continue[11].

Wintics, start-up parisienne qui travaille sur l'intelligence artificielle et le deep learning au service notamment de la mobilité urbaine explique assez bien cette technologie : « *Prenons l'exemple des faussaires de billets de banque traqués par les policiers. Le Générateur joue le rôle d'un faussaire qui produit une liasse de 100 faux billets de banque (dont les designs sont tous différents). Il la présente à un policier (le Discriminateur) qui, grâce à l'observation d'une base de données de billets authentiques qui lui a été transmise, a des connaissances basiques en identification de billets contrefaits. Le policier va donc analyser les billets du faussaire et les clas-*

ser en deux catégories : ceux qu'il pense être vrais et ceux qu'il pense être faux. À chaque fois qu'un faux billet est identifié par le policier, celui-ci est renvoyé au faussaire. Cela va permettre à ce-dernier de connaitre les designs qui n'ont pas été capables de tromper la police et par symétrie, ceux qui ont été assez réalistes pour passer à travers les contrôles. Par cette logique d'apprentissage, le faussaire va pouvoir créer de nouveaux billets plus réalistes et les représenter au policier. Celui-ci donnera une nouvelle fois son verdict et ainsi de suite. Le processus s'arrête lorsque le faussaire (le Générateur) est capable de créer des billets qui trompent le policier (le Discriminateur) à tous les coups »[12].

Les GAN peuvent ainsi par exemple faire évoluer des designs en fonction de contraintes physiques ou augmenter la résolution d'une image.

Et Wintics de conclure : « *Avec l'apparition des GAN, la Data Science s'est dotée d'un formidable outil de création et s'attaque ainsi à ce qui semblait être un des derniers prés carrés de l'intelligence humaine* ».

b. Holly GAN et jeu de dupes

Comme l'expliquait l'un des spécialistes belges de la question, Charles Cuvelliez, professeur à l'École polytechnique de Bruxelles (ULB), sur les ondes de la RTBF, les deepfakes peuvent être déclinés en trois catégories[13] :

01. Face Swapping : Qu'est-ce que mon visage fait sur ce corps ?

Fin 2017, un développeur, se faisant appeler Deepfakes sur le forum Reddit[14], avait réussi à insérer des visages de célébrités dans des films pornographiques. Il a ainsi conçu « *un programme capable d'automatiser ce processus, en se basant notamment sur une technologie d'IA*[15] *mise à disposition gratuitement par Google, nommée Tensorflow. Son système, "nourri" de centaines de photos et de vidéos de la star choisie glanées sur le Web, est ensuite capable de déformer suffisamment le visage d'une actrice de film pornographique pour qu'elle ressemble au modèle qu'a "appris" le programme* »[16]. Puis ce fut un autre internaute qui mit en ligne « *un programme similaire, ne nécessitant pas de compétences pointues. C'est alors l'emballement : les internautes s'emparent de ce logiciel nommé FakeApp, gratuit, et se mettent à publier en masse leurs créations, aidés par des modes d'emploi détaillés* »[17]. Au fil des expériences de chacun, le programme se perfectionne et des bases de données d'images de stars, indispensables à la création de ces vidéos, sont partagées. Car pour arriver à un résultat satisfaisant, il fallait disposer d'un grand nombre d'images, les personnalités publiques étaient donc particulièrement visées. Déjà « *en 2018 une entreprise du secteur avait même annoncé pouvoir insérer ses clients dans leurs vidéos favorites accompagnés des actrices "de leur choix"* »[18].

Entre de mauvaises mains il peut être destructeur

Le principe, appelé « face swapping » (échange de visages) ne se limitera bien sûr pas aux films érotiques ou pornographiques. Des visages, dans des scènes de films cultes, seront par exemple remplacés par d'autres et les déclinaisons vont se multiplier.

Et il ne faut pas aller jusqu'aux États-Unis pour trouver des amateurs de ce type de trucage vidéo. L'un des premiers deepfake de l'histoire aurait été fait en Belgique. Dans un reportage de M6 de mars 2019, l'Anversois Sven Charleer présente ainsi ses vidéos dans lesquelles il s'amuse à placer le visage de sa femme sur le corps de l'actrice américaine Anne Hathaway. Il déclare lui-même : « *C'est un outil très puissant, entre de mauvaises mains il peut être destructeur. Je pense qu'on ne réalise pas son pouvoir* »[19]. Heureusement les deepfakes qu'il réalise sont encore décelables pour qui s'y attarde un peu.

Puis la technique n'a cessé d'évoluer. L'application Zao a fait parler d'elle à l'été 2019. C'est une application mobile qui permettait de réaliser très facilement du *face swapping*. Il suffisait à l'application d'une seule photo de notre visage, ou d'une petite vidéo pour un meilleur effet, pour que notre tête soit transposée sur celle d'un acteur, dans une séquence vidéo déterminée, et ce en quelques secondes. Des millions de gens se sont ensuite amusés à placer des visages sur des clips, des films, des vidéos grâce à FaceApp, Zao, Morphin ou Reface app. Cette dernière application, lancée par l'entreprise ukrainienne Reface AI, a fait le buzz à l'été 2020. En quelques jours, elle s'est hissée à la première place du classement des meilleurs téléchargements sur le PlayStore. Il suffisait de faire un selfie et de sélectionner le clip dans lequel vous vouliez intégrer votre visage. Bien sûr ces quelques minutes d'amusement s'échangent contre une utilisation par ces sociétés, qu'elles soient chinoises ou ukrainiennes, des informations et photos fournies. De quoi fournir une belle base de données de reconnaissance faciale, mais c'est un autre débat.

Désormais, des sites comme Undress AI ou PTool proposent de placer des visages sur des photos de femmes nues. Des sites qui ventent leur facilité d'utilisation. Un jeu d'enfants. Nous verrons que cela peut représenter de sérieux dangers démocratiques et humains.

02. Ne me faites pas dire ce que je n'ai pas dit !

Ici, on ne se contente pas de mettre un visage sur le corps d'un autre, c'est le discours qui est modifié. L'une des premières techniques était celle du Lip sync, pour synchronisation labiale, qui consistait à ne modifier que les lèvres, et leurs contours, d'une personne pour les adapter à un autre discours. L'une des plus connues est celle où on voit Barak Obama insulter Donald Trump. Le trucage, révélé au public en avril 2018, a été fait par le réalisateur et comédien Jordan Peele, avec Adobe After Effects, un logiciel vidéo facilement disponible, et FakeApp. L'objectif poursuivi était d'éveiller les consciences aux problèmes des deepfakes[20].

Les hypertrucages ne sont bien sûr pas l'apanage de pirates. De nombreux débouchés leur sont trouvés comme corriger le bafouillement d'un acteur dans une prise de tournage ciné. Dès 2019, une équipe de chercheurs de l'Université de Stanford, de l'Institut Max Planck, de l'Université de Princeton et d'Adobe Research avait déjà mis au point « *une version simplifiée de ces trucages, avec l'aide des développeurs des logiciels Adobe* »[21]. À l'aide d'une vidéo existante et suffisamment longue de quelqu'un en train de parler, on peut donc lui faire dire d'autres choses de façon assez naturelle. Même des transitions de mouvements de mains ou de corps sont bluffantes. Pour les besoins de leur démonstration, les scientifiques ont transformé la célèbre phrase tirée du film *Apocalypse Now* « *j'aime l'odeur du napalm au petit matin* » en « *j'aime l'odeur du pain grillé au petit matin ». Impossible de distinguer l'original de la supercherie* »[22].

Falsifier une vidéo quasiment en direct

Plus fort encore, le « face2face » a permis, dès 2016 déjà, de falsifier une vidéo quasiment en direct. Grâce à l'approche conçue par des étudiants allemands et américains[23], on utilise un acteur source comme vous et moi pour faire faire les mêmes mouvements et expressions à une vidéo d'un acteur cible. N'importe qui peut ainsi servir d'acteur source pour faire faire des grimaces à une vidéo de Vladimir Poutine, par exemple. « *Il ne s'agit plus de coller son visage sur celui d'une star dans un blockbuster hollywoodien, mais d'animer le visage d'une personnalité avec des mimiques et des paroles inventées, ce qui pourrait par exemple permettre de produire une fausse conférence de presse d'un chef d'État, le tout en direct* », s'inquiète Camille Toussaint, journaliste à la RTBF [24].

Soulignons aussi l'arrivée d'Avatarify, un programme qui superpose le visage de quelqu'un d'autre au vôtre en temps réel, lors de visioconférences. Tout le monde peut ainsi avoir par exemple le visage d'Elon Musk pendant une conférence sur Zoom ou Skype[25].

Diverses technologies, susceptibles de faire gagner en qualité les deepfakes, évoluent ainsi en parallèle comme l'application Lyrebird qui développe son propre outil de clonage des voix[26]. En avril 2018, Lyrebird annonçait avoir développé une technologie d'intelligence artificielle capable d'imiter n'importe quelle voix en se basant sur un enregistrement « d'une minute seulement ».

Depuis, l'IA a révolutionné l'accessibilité aux deepfakes. Le célèbre ChatGPT a ouvert le bal et des applications comme Midjourney ou DALL-E ont connu un succès colossal. Nous n'avons pas tardé à voir de fausses images d'Emmanuel Macron en train de ramasser des poubelles dans Paris, du pape François en doudoune blanche ou encore de Donald Trump en tenue orange de prisonnier US. Des photos satiriques qui ont permis à beaucoup de monde de prendre connaissance du phénomène deepfake en Belgique, et ça n'est pas plus mal. On a pu voir également quantité de photos de quidams, sur lesquelles ils s'étaient transformés en rockeur, en viking, en personnage de série culte ou en train de faire un selfie avec Albert Einstein. Des applications plutôt ludiques de manière générale et essentiellement de photos. Car des sites nous proposent de créer nos deepfakes quasi en direct, comme Deep-Fake.ai qui nous annonce « *Deep-Fake.ai propose deux fonctionnalités intéressantes : l'image deepfake et la vidéo deepfake. Alors que la fonctionnalité d'image deepfake est déjà disponible, la fonctionnalité vidéo deepfake est actuellement en préparation et sera bientôt publiée. Restez à l'écoute pour cet ajout passionnant qui permettra aux utilisateurs de créer des vidéos deepfake réalistes et captivantes en un rien de temps* ».

Nous verrons par la suite les éventuels risques que cela peut représenter, notamment une fausse vidéo jointe à une fausse voix qui peuvent tromper bien des gens inattentifs.

03. Qui est cette personne ?

Certains se sont peut-être déjà amusés à chercher lequel des deux visages proposés en photo sur www.whichfaceisreal.com était réel. À chaque fois un des deux individus est créé de toute pièce. « *Les résultats du jeu Which Face Is Real ?, mis en ligne par deux professeurs de l'université de Washington, Jevin West et Carl Bergstrom, afin de tester la technologie de Nvidia, ne sont pas rassurants. Sur 6 millions de parties jouées par 500 000 personnes, le taux de réussite est de 60 % dès le premier essai mais ne dépasse pas 75 % avec de l'entraînement* »[27].

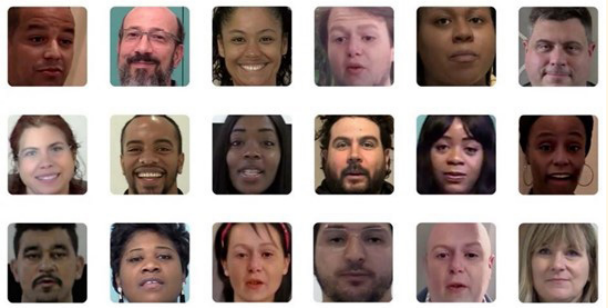


Image : Facebook (voir whichfaceisreal.com)

Et ces personnes ultra réalistes fabriquées de toutes pièces grâce au GAN, peuvent désormais être animées en vidéo. Et d'après Charles Cuvelliez, ce sont les deepfakes les plus difficiles à déceler.

2. Les débouchés du "faux profond"

La technologie de pointe derrière ces vidéos, a une gamme d'applications commerciales, en particulier dans les industries créatives telles que la publicité, le champ artistique ou la réalisation de films. Les publicités et les campagnes peuvent être plus facilement doublées, les contraintes de temps des acteurs peuvent être réduites et les effets spéciaux peuvent être créés plus rapidement et en toute sécurité. Des campagnes de sensibilisation peuvent également mettre en image une réalité future ou une situation hypothétique.

Citons cette jolie initiative du musée Salvador Dali de Floride qui a redonné vie à l'artiste espagnol sur écran pour accueillir les visiteurs. Le résultat est bluffant. On peut même faire un selfie avec lui[28]. Côté belge, on n'est pas en reste. Christopher Ume, et sa société Metaphysic, qui s'est fait connaître avec des deepfakes de Tom Cruise devenues virales sur Tik Tok[29], a créé l'événement en 2022 dans la célèbre émission de télé crochet américaine America's got Talent[30]. Il y a notamment fait chanter les membres du jury sur grand écran aux côtés d'Elvis Presley, le tout via la technique deepfake[31]. Le public et le jury ont adoré. Et il y a fort à parier qu'on reverra ce style de show mêlant des personnalités du passé à d'autres actuelles, voire même à des personnages tout à fait imaginaires. L'IA n'a pas fini de nous surprendre.

Mais d'étranges déclinaisons voient également le jour. Exemple récent, en février 2024, un article du journal *Le Monde* titrait « *TikTok et le business des récits de faits divers dopés au deepfake … Un visage, appartenant à une personne réelle ou fictive et animé par l'IA, vous fait de la voyance, raconte un fait divers glauque ou un récit incroyable. Le Monde a ainsi recensé une centaine de comptes TikTok spécialisés dans ce format, dont certains affichent plusieurs centaines de milliers d'abonnés, et des vidéos en français, arabe, anglais, espagnol, allemand ou italien qui cumulent parfois des millions de vues* »[32]. Le deepfake est ainsi utilisé pour ajouter de la crédibilité au récit. Voir un criminel raconter ses horreurs paraît ainsi intéresser les amateurs du genre, même si cela reste une initiative quelque peu glauque.

« *TikTok travaille également sur une nouvelle option qui permettrait aux marques de déployer des influenceurs virtuels pour promouvoir leurs articles. Ces derniers seraient en mesure de vendre les produits via des vidéos et des diffusions en direct* »[33]. Mais cette tendance semble mieux acceptée par les consommateurs asiatiques qu'européens, pour le moment.

Le deepfake est ainsi utilisé pour ajouter de la crédibilité

Il faut dire que des deepfakes, présentateurs de journaux télévisés ou influenceurs créés de toute pièce peuvent travailler vingt-quatre heures sur vingt-quatre sans se fatiguer. La technique peut également rendre les jeux vidéo hyperréalistes et plus immersifs. Avoir son visage sur un héros de jeu pourfendant le mal sera certainement prisé par les amateurs. Ces personnages pourraient même être transposés à nos profils sur les réseaux sociaux, donnant une image idéalisée de ce que nous voulons montrer de nous.

Du côté de la mode et des achats en ligne, les débouchés sont nombreux. Vous pouvez essayer virtuellement les articles qui vous plaisent. « *Afflelou, Optic 2000 ou encore Atol offrent à leurs clients la possibilité d'essayer leurs lunettes depuis chez eux. De son côté, l'entreprise SuitUs propose une cabine d'essayage en ligne pour les marques de vêtements. Cette technologie crée un double corporel pour diminuer de 50% le nombre de retours lié au e-commerce* »[34].

Si les possibilités utiles sont nombreuses, nous allons nous intéresser à présent aux divers dangers que peuvent représenter les hypertrucages.

3. Quelques dérives pour la navigation

Le succès des fake news sur le net a surpris par son ampleur et par l'irrationalité de nombreuses d'entre-elles. Des réactions émotionnelles ont permis à certaines de faire un buzz à plusieurs millions de vues. Avec la possibilité de créer de la vidéo et du son, beaucoup craignent encore plus les dérives à l'échelle de la planète,

qu'elles soient sociétales (incitations au désordre social, influence sur les pratiques et les pensées des citoyens), criminelles (la falsification de preuves, l'extorsion, la fraude ou encore les problèmes de droits d'auteur), sociétales (harcèlement, l'intimidation). Voici les scénarios de risques possibles, certains plus réalistes que d'autres. À chacun d'en juger.

a. Nouveaux marchés et appâts du GAN

Qui dit nouvel outil, dit nouvelles possibilités. Parmi celles-ci, se trouvent souvent des moyens de se faire de l'argent illégalement ou d'être tenté de flirter avec des lois inadaptées et/ou archaïques.

01. Faire du clic, faire du fric

Pour l'instant, il s'agit surtout d'amusement, en mettant par exemple le visage de Silvester Stallone sur le corps d'Arnold Schwarzenegger ou celui de Di Caprio sur notre propre corps.

Mais, à l'instar des fake news, on peut aisément imaginer des deepfakes créés pour faire du clic[35] sur le dos de personnalités, et donc ramener des revenus publicitaires intéressants tout en profitant d'un bon référencement sur Google. On a ainsi vu nombre de fake news être bien plus rentables que des vraies dans le domaine politique. Des vidéos, sorties de leur contexte, ont ainsi surfé sur la polarisation des débats sur les réseaux sociaux et connu un gros succès. Pendant la campagne présidentielle américaine de 2016, n'a-t-on pas vu Paul Horner, appelé le roi des fake news[36], avouer détester Trump, tout en propageant nombre d'absurdités à propos d'Obama ou d'Hillary Clinton ? Son explication était simple, pour lui les anti-Démocrates étaient ceux qui relayaient le plus d'infos sans les vérifier[37]. Il produisait donc les infos qui rapportaient et tant pis si des gens étaient assez idiots pour les croire. Pour lui, il n'y avait pas d'intention de nuire dans ses actes. On peut imaginer une transposition du phénomène, faux audios et/ou vidéos à l'appui.

D'ailleurs on a aussi pu voir, début 2023, dans un hypertrucage devenu viral (10,5 millions de vues), Elon Musk avouer, face caméra, s'être drogué et expliquer être prêt à imaginer de « *nouvelles voitures spatiales* » et à conquérir Mars[38]. C'était en fait un canular d'un habitué du genre, lancé sur Twitter, qui aura quand même fait 7,5 millions de vues. Mais combien de personnes y auront cru, impossible de le savoir. Le plaisantin aura en tout cas fait le buzz et un peu d'argent.

Par ailleurs, les influenceur·se·s deepfakes permettent d'aller encore plus loin pour vendre et attirer des followers. Début 2024, on a beaucoup parlé d'Adrianna Avellino, influenceuse générée par une intelligence artificielle (IA). Elle cumulait plus de nonante-quatre mille abonnés sur son compte. Sur son profil, un lien vers une page Fanvue, concurrent d'Onlyfans, avec des photos d'elle dénudée, moyennant un abonnement de cinq dollars par mois. Pour ce faire, « *selon le média américain 404media, des dizaines de vidéos d'utilisatrices Instagram ont été volées sans leur consentement et détournées pour remplacer leur visage, par celui d'Adriana. Avec, à la clé, des millions de likes et d'abonnés* »[39]. Des cas qui se multiplient avec des comptes totalisant des centaines de milliers de followers et des millions de vues, « *en utilisant "presque exclusivement" du contenu volé. Selon le média américain Manofmany, les influenceurs IA gagnent en moyenne 3.200 à 11.000 dollars sur Onlyfans* ». Des deepfakes tellement bien réalisés qu'ils sont devenus difficiles à détecter pour les followers. Et quand ces comptes sont signalés, puis supprimés par les plateformes, d'autres apparaissent rapidement.

Il est à parier que, pour faire de l'argent, nombre d'idées vont encore voir le jour, deepfakes à l'appui.

02. Manipulations, abus de confiance, vols d'identité et autres arnaques

Durant la pandémie de Covid-19, les solutions numériques aux problèmes ont explosé et, par la force des choses, la fraude en ligne aussi. La démocratisation des deepfakes a provoqué un boum des manipulations et des arnaques. Imaginez, par exemple, un parent recevoir un coup de fil de son enfant en difficulté et qui a besoin qu'on lui envoie de l'argent immédiatement. Par ailleurs, un militaire ou un employé pourrait-il refuser d'obéir à l'ordre d'un faux supérieur hiérarchique en vidéo conférence ? L'exemple, bien que déjà ancien, de Gilbert Chikli est significatif dans ce cas de figure. En 2005-2006 l'homme s'est fait passer pour le PDG de grandes entreprises auprès de cadres et leur demandait, par téléphone, de lui transmettre des centaines de milliers d'euros. Il a ainsi réussi à dérober plusieurs millions d'euros à des dizaines de grands groupes bancaires et industriels. Appelé « arnaque au président », la technique a fait de nombreux émules depuis, révolution de l'IA et imitation de voix deepfake à l'appui. Et en mars 2019, le *Wall Street Journal* annonçait que des criminels avaient utilisé pour la première fois un logiciel basé sur l'intelligence artificielle pour usurper l'identité d'un chef de direction et exiger un transfert frauduleux de 220 000 euros[40]. Début 2020, ce sont trente-cinq millions de dollars qui semblent avoir été dérobés à une banque émiratie de Hong-Kong[41]. Faux mails, faux papiers, et surtout… fausse voix de

directeur d'entreprise simulée par ordinateur. Plus fort encore, et toujours à Hong-Kong, début 2024 : le salarié d'une grande multinationale reçoit un mail de son directeur financier, basé à Londres, lui demandant d'effectuer de gros transferts. L'employé est méfiant mais sera vite rassuré par une visioconférence dans laquelle il reconnaît ses collègues et effectuera pour vingt-six millions de dollars de transferts. On s'apercevra qu'il avait parlé à … des avatars. Les fraudeurs avaient trouvé des vidéos et des audios accessibles au public via YouTube, puis utilisé les technologies deepfake et IA pour imiter leurs voix.

On a vu pendant la pandémie le nombre d'arnaques, d'hameçonnages et autres usurpation d'identité se multiplier sur le net. Les hypertrucages et l'IA ont considérablement perfectionné leur crédibilité apparente.

Le phénomène des *brouteurs*[42], qui font de l'arnaque aux sentiments, souvent depuis l'Afrique, pourraient avoir de beaux jours devant lui avec les deepfakes. Se faire passer pour quelqu'un d'autre devient de plus en plus facile. Un homme inscrit dans un CPAS hennuyer, nous expliquait récemment avoir perdu près de mille euros en croyant parler à une ravissante jeune femme, alors qu'il était dans une détresse affective, suite à un divorce.

Désormais les usurpations d'identité sont légions. Des personnes se font soutirer de l'argent en pensant avoir affaire à Florent Pagny ou à Conner Rousseau. Deux espagnoles ont ainsi perdu 325 000 euros, pensant entretenir une relation privilégiée avec Brad Pitt. Les malfrats avaient profilé et ciblé les deux femmes. Ils ont heureusement été arrêté mais ce qui interpelle, c'est que *« Pour trouver leurs victimes, les cybercriminels ont étudié les réseaux sociaux des femmes. Ils ont même dressé un profil psychologique d'elles … Ils ont découvert que les deux femmes étaient des personnes vulnérables, en état de dépression et en manque d'affection »*[43]. Deepfakes et profilages rendent désormais l'arsenal des escrocs particulièrement efficace et déstabilisant.

Le principe flirte avec l'usurpation d'identité

03. Droits d'auteur, comme de faux airs de faussaires

C'est l'un des grands débats du moment. Utiliser le deepfake pour imiter la voix, parfois avec l'image en plus, d'une chanteuse ou d'un chanteur, en a fait bondir quelques-uns dans le monde musical. Le 14 avril 2023, on découvrait sur YouTube, TikTok et d'autres plateformes, la chanson *Heart on my sleeve*, chantée par les Canadiens Drake et The Weeknd. Elle a rapidement fait le buzz le temps d'un week-end, *« avant que les artistes concernés et leur maison de disques, Universal Music Group, dénoncent un "fake" et obligent les plates-formes à le retirer dare-dare. Une contrefaçon confirmée au même moment par un faussaire anonyme, du nom de Ghostwriter977, écrivant dans un commentaire vidéo avoir utilisé l'intelligence artificielle (IA) pour générer les voix des deux vedettes. "J'ai été pendant des années auteur anonyme payé des clopinettes pour le plus grand profit des majors. Voici l'avenir", narguait-il »*[44]. Depuis, les plagiats n'ont plus cessé, d'Angèle à Jay-Z, jusqu'à faire revivre des chanteurs décédés comme Frank Sinatra ou Michael Jackson. Comment gérer les droits d'auteur d'un·e chanteur·se si sa voix et son style sont plagiés par quiconque ? On peut éventuellement entendre le côté amusant de la parodie, et imaginer faire danser et chanter *La danse des canards* à Taylor Swift, mais faire un gros succès sur les réseaux avec une fausse chanson de Billie Eilish. Le principe flirte avec l'usurpation d'identité.

Au-delà du côté divertissant, *The Guardian*[45] s'interroge sur les conséquences de ces deepfakes pour l'industrie musicale. Car OpenAI est loin d'être le seul acteur à s'intéresser aux algorithmes générateurs de musique. Google a créé en 2016 le projet Magenta, dont le but est de mettre au point des intelligences artificielles créatives. Spotify s'est doté d'un Creator Technology Research lab, à l'origine de « Hello World », premier album composé avec une IA. En 2023, des fans d'Oasis, fatigués d'attendre une réconciliation des frères Gallagher et une reformation du groupe, ont tout simplement sorti eux-mêmes un album intitulé *AIsis* (Contraction d'Oasis et de AI) : *The lost tapes*, et produit à partir de mélodies emblématiques de Liam Gallagher et de voix générées par ordinateur[46]. Les fans sont ravis mais les Gallagher peuvent-ils réclamer des droits d'auteur sur cette imitation, respectueuse du travail des deux frères ennemis ?

Et puis, si les stars ont les moyens de lancer des poursuites judiciaires, les artistes moins connus ne risquent-ils pas de se faire plagier facilement ? Sera-t-il encore judicieux de mettre sa maquette ou son morceau en ligne pour se faire connaître sans risquer de se la faire voler ?

Aujourd'hui, avec l'IA Uberduck, vous choisissez la voix d'une star de la musique puis vous saisissez le texte qu'elle doit prononcer et le tour est joué. Il faut juste promettre que ça ne sera pas utilisé à des fins commerciales.

À terme, chacun pourrait se créer sa, voire ses, propre·s chanson·s. Ou l'IA pourrait carrément vous créer une chanson personnalisée en fonction de votre humeur, ce qui est désormais réaliste au vu des masses de données de plus en plus disponibles pour alimenter les algorithmes d'apprentissages ? Les possibilités sont tellement vertigineuses, qu'il est difficile d'anticiper les réactions

et acceptations du public, auxquelles s'adaptera inévitablement l'industrie et la technologie IA. Il faudra légiférer en conséquence mais ça ne sera pas simple au vu des évolutions permanentes.

04. Le Métavers, allégorie de la grotte platonicienne 3.0. ?

En 2021 était lancé le Métavers de Mark Zuckerberg, qui nous avait imaginé un monde virtuel avec des avatars et une économie parallèle où on pouvait s'acheter une maison ou des NFT (œuvres virtuelles), se faire de nouveaux amis et épater la galerie à grand renfort de bitcoins. Mais ce concept élaboré en 1992 par Neal Stephenson, dans le roman de science-fiction *Le Samouraï virtuel*, un livre culte pour les entrepreneurs de la Silicon Valley, fut un flop retentissant pour Mark Zuckerberg. Cela dit, à ce jour, plusieurs centaines de métavers peuvent déjà être recensés et les plus grands (Roblox, Second Life, Zepeto, Minecraft, Fortnite) regroupent des millions d'utilisateurs.

Le concept est aussi vague que fourre-tout. Le rapport interministériel français de la mission sur le développement des métavers, publié en octobre 2022[47], définit ce dernier comme « *un service en ligne donnant accès à des simulations d'espaces 3D en temps réel, partagées et persistantes, dans lesquelles on peut vivre ensemble des expériences immersives* ». Malgré l'échec de Meta, l'idée persiste et de nombreuses entreprises comme Microsoft, Amazon ou Google investissent dans le concept. Un rapport récent du cabinet McKinsey évalue à cinq mille milliards de dollars le marché du métavers à l'horizon 2030, soit l'équivalent de la troisième économie mondiale derrière les États-Unis et la Chine. Les investissements sont évalués à plus de cent vingt milliards de dollars. Le projet métavers dépasse les ambitions d'une seule entreprise, aussi grande soit-elle … de grandes marques, comme « *Nike, Balenciaga ou Louis Vuitton se sont positionnées dans ces espaces virtuels* »[48]. De son côté Mark Zuckerberg n'envisage pas le Métavers rentable avant 2030.

Ces projets permettraient de créer une économie parallèle, en bitcoins, difficile à surveiller pour les États, et de se créer une vie parallèle « plus fun » dans laquelle les deepfakes et l'IA auraient une grande place à jouer. Une belle opportunité pour se faire connaître, que l'on soit une grande marque ou un artiste inconnu. D'autres y voient carrément l'avenir du télétravail[49]. En tout cas, le concept ne séduit pas encore beaucoup de monde, il est d'ailleurs encore assez méconnu voire flou.

La dépendance à ces vies virtuelles, au détriment d'une vie sociale

Mais n'est-il pas plus simple de jouer à un jeu vidéo immersif avec un casque de réalité virtuelle ? D'autant que ces mondes parallèles du Métavers risquent d'augmenter un peu plus la dépendance à ces vies virtuelles, au détriment d'une vie sociale et d'une économie locale. Sans compter que la plongée dans ces univers trop parfaits peut entraîner déception, voire dégoût de son physique et de sa propre personne, des dérives déjà observées sur Instagram et sur TikTok[50]. Sans parler de la perte de perceptions des expressions faciales des autres êtres humains, par exemple et de l'empathie. Dans son fameux livre, *Alone together* (*Seuls ensemble*, L'Echappée, 2015), la chercheuse Sherry Turkle, psychologue et professeur au Massachusetts Institute of Technology, constate que la connexion incessante avec les robots et les ordinateurs dévore les relations humaines en face-à-face et affaiblit l'empathie[51].

Si le métavers devenait une réalité, il pourrait accélérer la déliquescence du tissu social, affaiblir l'empathie humaine et nous conduire à rêver notre vie plutôt que de la vivre vraiment et rompre les liens sociaux qui sont une des bases fondamentales de notre humanité.

05. Quand l'IA nous relia, jusqu'à ce que sa mort nous sépare

L'IA permet désormais, grâce aux milliers de données laissées sur le net par un proche, de faire « revivre » celui-ci après son décès. Le thème de l'immortalité est un vieux fantasme et le deuil d'un être cher est une des choses les plus difficiles à accepter, il suffit de voir le succès de certains voyants communiquant avec les esprits. Le sujet est pernicieux car, converser avec un aïeul pour comprendre ses racines peut être vraiment intéressant. C'est ce que propose HereAfter AI, une société basée aux États-Unis qui permet aux gens de « *télécharger leurs souvenirs, qui sont ensuite transformés en un "avatar d'histoire de vie" avec lequel les amis et la famille peuvent communiquer* »[52]. Cette méthode permet aux gens de laisser leurs souvenirs pour les générations futures. Mais que les datas laissées sur le net soient représentatives de qui était la personne semble excessif. N'oublions pas que, comme le précise Amélie Cordier, ingénieure et maîtresse de conférences en intelligence artificielle à l'Université Lyon I : « *On prête à l'intelligence artificielle des idées, des pouvoirs, des applications qui ne sont en fait ni plus ni moins que des désirs, des vœux d'êtres humains. Le mot important dans tout ça, c'est "simulation". Avec ces intelligences artificielles génératives, qu'on n'avait pas jusqu'à maintenant, effectivement, il est possible de simuler le fait qu'une personne que l'on connaisse puisse parler. Et l'IA permet de faire ça avec une qualité de simulation qui est vraiment très intéressante. Mais ce n'est ni plus ni moins la même chose que de se dire : "Je vais parler avec un personnage de jeu vidéo"* »[53].

Pour le « *Dr Kirsten Smith, chargée de recherche clinique à l'Université d'Oxford, le risque est que ces avatars de défunts nous maintiennent accrochés au passé, nous rendent incapables d'aller de l'avant et de mener normalement notre vie* »[54]. Le danger de conséquences psychologiques est bien réel.

Autre manière de prendre ses simulations pour des réalités, en 2022, une femme de quatre-vingt-sept ans a carrément assisté à ses propres funérailles au Royaume-Uni, grâce à une startup appelée StoryFile, qui enregistre des séquences vidéo et audio avant le décès d'une personne. Elle les rend ensuite interactives grâce à la puissance de l'intelligence artificielle et d'un avatar holographique[55].

Au royaume de l'IA et du deepfakes, la fantaisie humaine semble être un bel exemple de l'infini.

b. Enjeux de société

01. Le faux pour secouer le vrai

Diverses associations ont aussi compris tout l'intérêt des hypertrucages pour des campagnes de sensibilisation dites positives.

Exemple chez nous, en mars 2020, avec un discours vidéo fictif de Sophie Wilmès publié sur les réseaux sociaux pour relancer les actions du groupement d'activistes écologistes Extinction Rebellion. La Première ministre y déclarait : « *La pandémie actuelle de Covid-19 plonge ses racines dans la destruction écologique mondiale et ce sont les plus vulnérables dans nos sociétés qui sont le plus durement frappé·e·s* ». Une vidéo qui a été largement diffusée sur les médias sociaux et dans les médias *main stream*, sans doute en raison de sa nouveauté et de son originalité. En effet, jamais on n'avait détourné la vidéo d'un ou d'une Premier·e ministre belge via un deepfake, d'autant que le message allait plutôt à l'encontre du discours plutôt libéral de celle-ci. L'objectif a donc été atteint pour l'association écologiste.

Ces campagnes de sensibilisation dites positives sont aussi accusées de jouer avec le feu. En octobre 2019, l'association Solidarité Sida a mis en ligne une vidéo du président des États-Unis Donald Trump. « *Le sida, c'est fini* », semble déclarer ce dernier. Mais, il s'agissait en fait d'un acteur dont le visage avait été numériquement modifié pour laisser entrevoir la possibilité d'un « monde sans sida », comme l'explique Antoine de Caunes, le président d'honneur de l'association, à la fin de la vidéo. Beaucoup d'internautes s'y sont cependant laissé prendre et ont critiqué une campagne qui joue avec les limites du réel à des fins de communication. Le clip a été vu 3,5 millions de fois en quelques heures et a sans doute touché son public cible : les jeunes. Le directeur fondateur de l'association Solidarité Sida, Luc Barruet, prête à cette vidéo truquée « *des vertus pédagogiques, pour que les gens mesurent ce que l'on peut faire avec les deepfakes* »[56]. À ses yeux, les critiques émises sur le Net, quant au caractère « *douteux* » ou « *dangereux* » de cette fausse vidéo dont il faut attendre la fin pour en comprendre le sens, sont peu nombreuses en comparaison de son succès viral, précisant que « *ceux qui réagissent sur les réseaux sociaux sont toujours ceux qui ne sont pas contents, pas ceux qui trouvent ça formidable* »[57].

L'intérêt des hypertrucages pour des campagnes de sensibilisation

Le deepfake peut ainsi être très utile pour éveiller les consciences sur différents sujets mais ces vidéos fabriquées peuvent se retourner contre l'intention de départ ou être sorties de leur contexte initial, en tout ou en partie. Ainsi en 2018, en Inde, une vidéo a longtemps circulé dans tout le pays et effrayé les Indiens. « *Elle montre deux hommes à moto qui s'approchent d'un groupe d'enfants qui jouent au cricket. La moto ralentit, le passager attrape l'un des enfants et ils prennent tous deux la fuite. Un procédé rapide et terrifiant. Sauf que cette vidéo ne décrit en aucun cas un fait réel. C'est même l'opposé : ce clip fait partie d'une campagne de prévention contre les enlèvements d'enfants, et pas en Inde, mais au Pakistan. (…) La vidéo a circulé sur WhatsApp et dans l'État du Goujarat, à l'ouest du pays, accompagné du message d'alerte suivant, prétendument issu par la police : "un gang de 300 enleveurs d'enfants est arrivé dans la région, protégez vos enfants !"*[58] ». Des dizaines de personnes suspectées d'être kidnappeurs ont été tabassées par la population et de janvier à juillet 2018, une trentaine de personnes sont mortes, lynchées par des foules. La police a été dépassée par le phénomène, d'autant que l'info a été diffusée sur WhatsApp, qui est une messagerie cryptée et donc quasiment impossible à intercepter. Un simple détournement d'une vidéo de sensibilisation sur fond de tension sociale aura ainsi provoqué plusieurs dizaines de morts.

Une multiplication excessive de vidéos fictives pourrait également desservir la cause s'il n'est pas précisé systématiquement à l'image que la vidéo est un faux. Mais cela peut être camouflé pour être détourné, à l'instar de cet exemple indien.

02. Satires à tout va

Il est certain que le deepfake est une magnifique opportunité pour tous de faire de la satire. Elle sera de bon ou de mauvais goût et elle sera différemment acceptée selon son point de vue. À l'instar du deepfake qui a fait danser la princesse Leonor, héritière d'Espagne, sur TikTok. Beaucoup y ont cru et ont ensuite

trouvé la blague de mauvais goût car l'utilisation de l'image de la princesse avait été réalisée de manière trompeuse. Il aurait mieux valu souligner qu'il s'agissait d'un faux.

Et encore, lorsque la chaîne de télévision britannique Channel 4 suscite la controverse à Noël avec une vidéo « deepfake », diffusée vendredi 25 décembre, qui tourne en dérision le traditionnel discours de la reine Elizabeth II et le font terminer par un jerk endiablé de la Reine[59], les sujets de Sa Majesté ont crié à l'outrage, malgré les bonnes intentions clamées par la chaîne.

À l'heure où n'importe qui peut se prendre pour un caricaturiste de *Charlie Hebdo*, nul doute que la justice de nombreux pays va avoir fort à faire dans les prochaines années pour trancher et fixer les limites de l'amusement et de l'humiliation. Enfin, si elle en reçoit les moyens.

03.Je jure de dire la vérité

Au niveau judiciaire, la notion de preuve risque d'être quelque peu ébranlée. Ainsi, le premier cas de deepfake invoqué dans un procès en France, l'a été par le célèbre humoriste polémique Dieudonné. Dans une vidéo, publiée le 8 avril 2020 sur YouTube puis retirée, on le voyait critiquer vigoureusement les réquisitions d'une magistrate de Nanterre, la comparant notamment aux femmes ayant collaboré avec le régime nazi. Pour sa défense, il avait déclaré que cette vidéo était un deepfake. « *Aujourd'hui, avec les deepfake, l'image n'est plus une preuve* », avait plaidé son avocat David de Stefano, demandant sa relaxe. La cour a finalement quand même condamné Dieudonné à trente mille euros d'amende ne jugeant pas cet argument crédible.

À l'inverse, ce faits-divers, aux États-Unis, qui souligne combien le deepfake s'immisce dans toutes les sphères de nos sociétés. Raffaela Spone est accusée d'avoir harcelé trois adolescentes, à l'aide d'images manipulées, pour leur faire abandonner leur rôle dans l'équipe locale de *cheerleading* (l'équipe de supportrice) du comté de Bucks en Pennsylvanie. La mère de famille encourait jusqu'à un an de prison et les médias ont largement contribué à populariser l'affaire. Après presqu'un an de procédure, Matthew Weintraub, le procureur du district du comté de Bucks a annoncé abandonner les poursuites contre Raffaela Spone, la police ayant été incapable de fournir les preuves d'une quelconque manipulation de la vidéo.

Prouver, de manière irréfutable, qu'un faux est faux

Faudra-t-il bientôt prouver, de manière irréfutable, qu'un faux est faux et qu'un vrai est un vrai ? La justice n'a pas fini de devoir adapter les lois à ces nouvelles technologies, en mutation perpétuelles.

04.À chacun son Histoire

Un outil deepfake, permettant aux utilisateurs d'animer d'anciennes photos de proches, a été largement utilisé sur le site MyHeritage, site de généalogie permettant de retrouver ses aïeux. Au vu du succès, le site a désormais ajouté LiveStory, qui permet d'y insérer des voix.

En télévision, Thierry Ardison propose des interviews d'artistes décédés comme Dalida ou Jean Gabin grâce aux hypertrucages et au talent de comédiens.

Ces exemples soulignent qu'on pourrait tenter de faire croire qu'une personnalité n'est pas morte à l'aide d'une fausse vidéo, du moins pendant quelques temps. Pourrait-on aussi faire dire n'importe quoi au passé ? Sans aucun doute. La preuve ? En juillet 1969, en cas d'échec tragique de la mission lunaire Apollo 11, le président américain Richard Nixon avait prévu un discours. Des chercheurs du Massachusetts Institute of Technology (MIT)[60] en ont fait une vidéo[61]. Objectif : démontrer les dangers des hypertrucages, qui permettent de faire dire à une personne des mots qu'elle n'a jamais prononcés. Cette expérience montre ainsi qu'on peut imaginer un faux discours de Nixon prétendant qu'Armstrong et Aldrin n'ont jamais mis le pied sur la lune et il est fort à parier que la vidéo serait largement partagée au regard du nombre de sceptiques face à ce moment de l'histoire. Une enquête IFOP[62] a ainsi démontré qu'en 2019, un Français sur dix croyait que les Américains n'avaient jamais marché sur la lune.

Nos sociétés ne se construisent-elles pas sur des mythes fondateurs comme le fait que Charlemagne aurait inventé l'école ou que son ami Rolland aurait été tué par des Sarrasins, alors que c'était par des Basques. Et que dire de « Nos ancêtres les Gaulois », idée répandue aux XIXe et XXe siècles par les nationalistes français, à une époque où les peuples d'Europe cherchaient à se donner une ascendance antique, pour justifier l'existence de leur État-Nation. Mais ces mythes étaient fondateurs d'un pays, d'une population acceptant de vivre ensemble et de croire en un récit commun, et non d'une vague croyance partagée par des personnes éparpillées aux quatre coins du monde et sans aucune cohérence existentielle.

En fait, les deepfakes risquent bien d'alimenter les prétendues preuves des complotistes et des négationnistes de tout bord, qu'elles soient sonores, scripturales ou visuelles.

05. Pour le journalisme, un risque d'y perdre des plumes

Au-delà de la difficulté pour les journalistes de dénouer le vrai du faux avec l'arrivée des deepfakes et de l'IA, comme nous le verrons plus tard, les hypertrucages peuvent devenir une tentation professionnelle pour ceux-ci. L'IA est effectivement de plus en plus utilisée par les journalistes, notamment pour la retranscription ou la traduction d'interviews ou encore pour une aide à la rédaction, à la correction des articles, au résumé ou à l'analyse de dossiers complexes. Mais à vouloir gagner du temps, ils doivent faire attention à la limite, parfois fragile, entre « les super assistants » et la manipulation.

En Belgique des journalistes débattent sur le sujet. Selon Yves Thiran, journaliste et membre d'un groupe de réflexion sur ces nouvelles technologies au sein de la RTBF, interrogé par Martin Bilterijs : « *C'est tout ce qui est la production de contenus. Que ce soit du contenu sous forme de texte, d'image ou de vidéo. A la RTBF, on s'abstient pour l'instant. Mais on voit bien que d'autres médias ont déjà commencé, notamment quand il s'agit d'illustrer un article sur un site web et qu'il n'y a pas l'image de l'événement. Traditionnellement, on utilise des images prétextes, mais là on demande à l'ordinateur de fabriquer l'image. C'est une des questions qu'on se pose : doit-on ou pas s'autoriser ce genre de productions ? … Un site américain a d'ailleurs dénombré "49 médias désormais entièrement automatisés". Des sites qui génèrent des articles entièrement créés par l'intelligence artificielle. Ce sont "des médias de niche pas encore de grands médias"*, précise Yves Thiran[63].

Par ailleurs, le choix d'une image réelle, pour illustrer un article, reste un choix rédactionnel, en fonction d'une volonté de sensationnalisme par exemple. Mais créer une image en fonction de ce qu'on connaît d'un événement peut devenir beaucoup trop subjectif.

Il est également difficile de reconnaître une photo hyper truquée, même pour des professionnels. On se rappelle de cette photo qui avait gagné le prix du Sony World Photography Awards en 2023, avant que l'artiste ne révèle qu'il s'agissait d'un deepfake[64]. Les journalistes doivent garder la capacité de ne pas être trompés par des images qui leurs seraient envoyées par de faux témoins d'un événement.

Mais n'oublions pas ce que nous entendons en atelier d'éducation permanente ou en formation. Les participants nous révèlent préférer les articles courts et faciles à comprendre, voire même ne sélectionner que les bonnes nouvelles. L'info tend à devenir irréversiblement un produit de consommation comme un autre pour de plus en plus de citoyens. Pourtant l'actualité est souvent complexe et nuancée et ne peut être une simple distraction. Les journalistes ont sans doute une carte à jouer en restant gages de qualité et de vérification des faits. Gageons qu'on leur en laisse les moyens car il est difficile d'imaginer que l'IA puisse complètement remplacer un journaliste, avec son talent de plume, sa créativité, son recul, son expérience, son humour, sa perception de la vérité, sa probité, son éthique, et tout ce qui fait l'âme d'un être pensant neutre et indépendant.

06. Humiliations des femmes, quand la honte changera-t-elle donc de camp ?

En matière de harcèlement, les deepfakes sont malheureusement plus efficaces qu'ailleurs, surtout envers les femmes. « *D'après un rapport de l'entreprise hollandaise de cybersécurité Deeptrace Lab, sur les 14.000 vidéos hypertruquées mises en ligne en 2019, 96% d'entre elles étaient à caractère pornographique… De nombreuses célébrités comme Billie Eilish, Emma Watson ou encore*[65] *d'autres streameuses de la plateforme Twitch en ont été les victimes. Car l'autre constat alarmant de Deeptrace Lab est que le deepfake pornographique cible exclusivement des femmes. Les deepfakes non pornographiques analysés sur YouTube contenaient, quant à eux, une majorité de sujets masculins* »[66]. Et pour les femmes, cela est souvent dévastateur.

Pour les femmes, cela est souvent dévastateur

En Belgique, nous sommes loin d'être à l'abri car les exemples se multiplient. Fin 2023, Julia, vingt-et-un ans, étudiante belge en marketing et mannequin semi-professionnelle, reçoit des photos d'elle nue, pour lesquelles elle n'a jamais posé. Les photos sont tellement bien faites qu'elle est abasourdie : « *J'avais déjà entendu parler des deepfakes et des deepnudes (…) Mais je n'en avais pas conscience plus que ça avant que ça ne m'arrive à moi. C'était un événement un peu anecdotique qui se passait dans la vie des autres, mais qui ne se passerait pas dans la mienne* »[67]. La jeune femme dépose plainte au commissariat. Il est vrai que des lois peuvent être invoquées, comme celles sur le voyeurisme et la diffusion non consentie, ou comme la directive européenne sur les violences faites aux femmes[68]. Mais on prévient Julia « *que le "parquet est débordé" et qu'il y a "très peu de chances" que sa plainte aboutisse* »[69]. Autre exemple, à la même époque, c'est Céline Van Ouytsel, miss Belgique 2020 qui en était victime : « *Je savais que cela se faisait parfois avec des stars de Hollywood très célèbres, mais je n'aurais jamais pensé que cela puisse m'arriver un jour. Comme quoi, cela peut arriver à n'importe qui…* »[70].

Aucune femme publique n'est à l'abri. C'est par exemple arrivé à la célèbre influenceuse française Léna Situation. Elle explique : « *Ils*

ont mis un screen du vlog[71] *et le reste du corps ne m'appartient pas. Et il y a tellement de meufs sur internet qui vivent ça. C'est vraiment dégueulasse. Ça fait longtemps que je n'ai pas eu un moment que j'ai kiffé en tapant mon nom sur les réseaux sociaux. De bon matin, voir ma tête sur un corps nu ?! »*[72]. Février 2023, dans un direct diffusé le 2 février dernier sur la plateforme Twitch, QTCinderella, une streameuse (une joueuse qui transmet et commente ses parties de jeux vidéo en direct) américaine de vingt-huit ans, revient en larmes sur le deepfake à caractère pornographique dont elle a été victime : « *C'est à ça que ressemble la douleur. Voilà ce que cela fait de se sentir violée, abusée et de se voir nue contre sa volonté partout sur internet* »[73]. Une victime australienne, va également déclarer à Euronews « *C'est une condamnation à vie … Elle peut détruire la vie des gens, leurs moyens de subsistance, leur employabilité, leurs relations interpersonnelles, leurs relations amoureuses. Et il y a très, très peu de choses que l'on puisse faire une fois que quelqu'un est pris pour cible* ».

N'oublions pas les dégâts collatéraux de ces images

Il y a, d'ailleurs, fort à parier que des cas de chantages risquent de se multiplier pour un certain nombre de quidams. Combien préféreront payer cent, deux cents voire trois cents euros plutôt que de voir circuler sur le net des *deep nudes* ou *deep porns* ?

Ironie supplémentaire, les deep nudes d'hommes sont non seulement rares, mais ils sont également de moindre qualité. « *Les algorithmes sont entraînés spécifiquement sur le corps des femmes … Cela révèle une inégalité plus profonde entre les sexes, un manque de respect pour les femmes et la violence sexuelle dans la société. La technologie ne fait qu'encourager l'objectivation des femmes. De plus, il ne s'agit pas toujours de satisfaire un fantasme. Une fausse vidéo porno peut aussi être utilisée pour réduire les femmes au silence* »[74]. Déjà, en 2018, l'histoire vécue en Inde par Rana Ayyub, a fait froid dans le dos des femmes engagées en politique indienne. Cette journaliste d'investigation a été la victime d'une vidéo « deepfake » à caractère pornographique qui a circulé sur les réseaux sociaux, notamment grâce à l'aide d'hommes politiques d'après une de ses sources. Très vite, elle reçoit des menaces de viol. Un tweet est diffusé sur les réseaux sociaux avec une capture d'écran de la vidéo et son numéro à côté, disant « *Salut, c'est mon numéro et je suis disponible ici* ». « *Les gens ont commencé à m'envoyer des messages WhatsApp me demandant mes tarifs pour le sexe* ». « *J'ai été envoyée à l'hôpital avec des palpitations cardiaques et de l'anxiété, le médecin m'a donné des médicaments. Mais je vomissais, ma tension artérielle a monté en flèche, mon corps avait réagi si violemment au stress* », a-t-elle déclaré[75]. « *Le pays tout entier regardait en boucle une vidéo porno que l'on m'attribuait et j'étais tétanisée* »[76].

> *"Si vous étiez le pire misogyne du monde, cette technologie vous permettrait de réaliser tout ce que vous voulez", a déclaré Mary Anne Franks, professeur de droit à l'Université de Miami et présidente de l'association Cyber Civil Rights Initiative dont la mission est de venir en aide aux personnes victimes d'abus sur Internet partout dans le monde*[77].

L'histoire de Rana Ayyub fait ainsi craindre le pire pour les femmes qui mènent des combats politiques et/ou idéologiques à travers le monde, notamment face à une misogynie persistante. Cela dit, les hommes risquent de ne pas être épargnés non plus, quand on sait qu'une vie ou qu'une carrière politique peut dépendre d'une vidéo, à l'instar de celle, à caractère sexuel et partagée sur les réseaux sociaux, qui a conduit le candidat français Benjamin Griveaux à renoncer à la mairie de Paris en février 2019 avant même que l'authenticité des images n'ait pu être prouvée. Un deepfake pourrait avoir cet effet.

Heureusement, des femmes sont prêtes à se battre pour faire évoluer les lois. C'est le cas de la présentatrice TV hollandaise, Welmoed Sijtsma, qui s'est retrouvée dans un deep porn. En novembre 2023, le tribunal d'Amsterdam a condamné son auteur, un homme de trente-neuf ans, à cent quatre-vingts heures de travaux d'intérêt général avec sursis[78]. Son père avait refusé de regarder la vidéo, de peur de garder ces images en tête. Car n'oublions pas les dégâts collatéraux de ces images sur l'entourage des victimes, lui aussi souvent désemparé et frustré par un sentiment d'impuissance face à un phénomène nouveau, violent et excessivement intrusif.

07. "Déshabillez n'importe qui, déshabillez les filles gratuitement"

Un tiers des élèves de la FWB serait concerné par le harcèlement, et un « programme-cadre » de prévention du harcèlement et d'amélioration du climat scolaire a été lancé[79]. Il est effectivement difficile de protéger les jeunes des messages de haine, des harcèlement ou encore des images pornographiques, voire pédopornographiques, tout comme des arnaques et des réseaux de propagandes mensongères. La mode depuis peu : les deep nudes dans les écoles. En Belgique, « *une dizaine de jeunes filles de 12 à 16 ans, élèves du collège Saint-Remacle de Stavelot, ont été victimes de deepfakes. Des garçons de leur école et d'autres établissements scolaires ont récupéré les photos qu'elles postaient sur les réseaux sociaux. En utilisant l'intelligence artificielle, ils ont modifié ces photos pour faire apparaître ces adolescentes entièrement nues. Les images ont ensuite été partagées sur Snapchat* »[80]. Une « nouvelle mode » qui tourne parfois au racket, au chantage et/

ou au rançonnage. D'autant que ces images sont d'une facilité désormais déconcertante à réaliser. « Déshabillez n'importe qui, déshabillez les filles gratuitement », c'est le slogan de l'application ClothOff, qui a fait parler d'elle en Espagne récemment. Elle permet aux utilisateurs « *de "déshabiller" n'importe quelle personne apparaissant dans la galerie de photos de leur téléphone. Il en coûte 10 euros pour créer 25 images de nus* »[81]. Une application qui a donné des idées de chantages à quelques ados d'une école d'Almendralejo, une ville du sud de l'Espagne, où une vingtaine de jeunes filles ont vu passer de fausses photos d'elles nues. En clair, si une adolescente ne payait pas une petite rançon, un faux nu d'elle était publié sur les réseaux. Un faux qui a des chances de devenir viral dans leur école, à minima. Ce cas est une *sextorsion* mais il peut tout à fait s'agir de revanche ou de volonté d'humiliation d'une jeune personne. Et quand il s'agit de jeunes, voire d'enfants, les lois y sont encore moins préparées. Dans une interview accordée à Euronews, relatant ces faits , Manuel Cancio, professeur de droit pénal à l'Université autonome de Madrid, « *souligne qu'il existe un vide juridique car l'utilisation du visage de mineurs sur des photographies porte atteinte à leur vie privée, mais lorsqu'il s'agit de crimes dans lesquels des images intimes sont diffusées, c'est l'image dans son ensemble qui porte atteinte à la vie privée* »[82] mais « *Comme elle est générée par deepfake, la vie privée de la personne en question n'est pas affectée. L'effet qu'elle produit (sur la victime) peut être très similaire à celui d'une vraie photo de nu, mais la loi est en retard* », ajoute-t-il. La loi, espagnole en l'occurrence, est en retard, une phrase qu'on a pas fini d'entendre. Ce cas de chantage entre ados, nous apprend également que la plus jeune des victimes n'avait que onze ans et combien la manière de qualifier les faits ne fait pas l'unanimité parmi les avocats : « *il peut s'agir de pédopornographie, de crimes contre l'intégrité morale ou de distribution d'images à contenu sexuel non consensuel* »[83].

L'année dernière, Child Focus a ouvert pour la première fois un certain nombre de dossiers sur les deep nudes. « *L'augmentation du phénomène nous inquiète, déclare Niels Van Paemel, conseiller politique. Grâce à notre service d'assistance téléphonique, nous recevons de plus en plus de questions de la part de jeunes sur des images truquées, qui se sont effectivement retrouvées dans les écoles. C'est le point de basculement que nous redoutions. Les deepnudes sont au carrefour du genre, de la cyberintimidation, de l'exposition (NDLR: diffusion numérique d'images privées sans autorisation dans le but de nuire ou d'humilier la personne représentée), de l'exploitation sexuelle et de la maltraitance des enfants. Tout y est réuni* »[84].

Nous le verrons plus loin des solutions existent mais sont complexes à mettre en place.

c. Nouvelles armes de persuasion massives

01. Crédibilisation de la caricature et discréditation du vrai

Les attaques et discréditations politiques se multiplient déjà dans le monde. On a vu passer une vidéo de Mauricio Macri, président argentin de 2015 à 2019, avec le visage d'Adolf Hitler[85] ou un faux d'Inés Arrimadas, membre du Parlement de la Catalogne, superposé sur une vidéo pornographique. Est-ce une déclinaison moderne de la caricature ? Non, car on joue ici sur un hyper réalisme avec lequel un dessin n'essaie pas de rivaliser. En revanche pourrait-on présenter la vidéo de M. Macri comme de la satire ? En mai 1968 ne voyait-on pas une affiche présenter A. Hitler derrière le masque de Charles De Gaulle ? Il s'agirait ici d'une opinion politique tandis que la vidéo d'Inés Arrimadas ne peut être considérée comme telle.

Où mettre la limite ?

En mai 2019 un « deepfake » peu sophistiqué, plutôt appelé cheapfake (un faux « bon marché »), avait fait parler de lui aux États-Unis. On y voyait la présidente de la Chambre des représentants américaine, et farouche opposante à Donald Trump, Nancy Pelosi parler avec un phrasé hésitant qui donnait l'impression qu'elle était passablement éméchée, droguée, malade, voire hébétée. Une vidéo qui a eu le temps d'être partagée trois millions de fois avant que le *Washington Post* n'ait le temps de comparer la vidéo avec l'original et de constater que les images avaient simplement été ralenties de 25 %. Même Rudy Giuliani, le propre avocat du président Trump, avait eu le temps de la partager[86]. Cela permet de souligner l'importance du « biais de confirmation » dans le phénomène des partages de vidéos truquées, même de façon grossière : lorsqu'une vidéo semble prouver quelque chose à laquelle ils croient déjà, les internautes penseront plus volontiers que la vidéo est réelle, ou n'en auront cure, et la partageront. Quand bien même une vidéo aurait été mise en ligne comme satire, au départ.

Mais si les deepfakes étaient plutôt rares dans les campagnes électorales jusqu'ici, l'année 2024 a vu la moitié de la planète aller voter et le nombre de deepfakes politiques se multiplier.

Aux États-Unis, ce sont des hypertrucages audios qui ont fait parler d'eux. Dès janvier, un étonnant appel automatique a été reçu par cinq mille électeurs du New Hampshire. « *Au bout du fil, la voix de Joe Biden qui, dans un message préenregistré, leur déconseillait d'aller voter aux primaires démocrates américaines du mardi 23*

janvier. "Votre vote fera la différence en novembre, pas ce mardi (…) Voter ce mardi ne fera qu'aider les républicains à faire réélire Donald Trump". C'était un faux : la voix de Joe Biden a été imitée par intelligence artificielle. Un deepfake politique qui a généré beaucoup d'émoi aux États-Unis ». L'auteur a été découvert un mois plus tard. Steve Kramer, consultant pour la campagne d'un rival de Joe Biden, s'est défendu en argumentant que son initiative avait justement pour objectif de mettre en lumière les dangers de l'intelligence artificielle en politique. « *C'était une façon pour moi de faire la différence, et ça a marché* », a-t-il déclaré à NBC. « *Pour 500 dollars, j'ai obtenu un effet équivalent à 5 millions de dollars* »[87].

Quelques mois plus tard c'est Elon Musk, ardent défenseur de Donald Trump qui partageait un deepfake de la candidate démocrate en train de dire des choses telles que « *Moi, Kamala Harris, je suis votre candidate démocrate à la présidence parce que Joe Biden a finalement révélé sa sénilité lors du débat* » contre Donald Trump, explique la voix générée par IA dans la vidéo. Dans cette campagne artificielle, l'on peut entendre la fausse Kamala Harris affirmer qu'elle est une « *recrue de la diversité* », qu'émettre la moindre critique contre elle est « *sexiste* » ou « *raciste* » et qu'elle ne connaissait « *rien à la gestion du pays* »[88]. La vidéo, qui arbore le logo « *Harris for President* », n'a jamais été signalée par Elon Musk comme étant générée par l'IA. L'affaire a remis au premier plan la responsabilité des réseaux sociaux dans la diffusion de ces contenus. Surtout que X déclare interdire « *le partage de médias synthétiques, manipulés ou hors contexte qui peuvent tromper ou dérouter les gens et entraîner des préjudices* », à l'exception des mèmes et de la satire « *à condition qu'ils ne provoquent pas de confusion significative quant à l'authenticité des médias* ». Même pour de la satire, il semble tout à fait déplacé d'utiliser une vidéo d'une personne sans son consentement, surtout avec une vidéo hyperréaliste.

À la veille des élections présidentielle, les autorités américaines ont pris très au sérieux ce genre d'affaires. Tout comme en Europe, comme nous le verrons plus loin.

Il faut dire qu'aux États-Unis, des clans complotistes s'affrontent. Les Q-Anon, sympathisants de Trump, qui croient que des personnalités influentes sont impliquées dans des réseaux pédophiles internationaux, qu'elles veulent créer un nouvel ordre mondial dans lequel les États auraient abandonné leur souveraineté au profit de cette élite, et que seul Donald Trump pourrait les contrer, s'il est réélu. Comme réponse à l'absurdité de cette théorie, des sympathisants démocrates ont aussi créé une mouvance complotiste appelée BlueAnon, qui s'approprie l'univers et les codes de QAnon tout en inversant la cible. Ils entendent ainsi Lutter contre « *l'État profond* »[89] qui veut « *détruire la candidature du président Biden* » (de Kamala Harris désormais) et « *ramener Trump au pouvoir le 5 novembre* ». Affirmant que les médias refusent de relayer des révélations contenues dans de nouveaux documents rendus publics, impliquant Donald Trump dans le réseau de trafic sexuel de mineures du financier et prédateur sexuel Jeffrey Epstein. Le tout étayé par … une photo deepfake. Quelques incohérences au niveau des doigts de certaines mains et de la longueur du bras de la jeune fille de gauche ont confirmé qu'il s'agissait bien d'un deepfake.

Image deepfake, produite par les BlueAnon afin de discréditer Donald Trump et le camp des QAnon. La guéguerre entre complotistes risque d'alimenter les réseaux sociaux en deepfakes.

Côté européen, à l'approche des élections de 2024, on a pu découvrir Amandine Le Pen et Léna Maréchal sur TikTok. Deux sympathiques avatars sexy avec les visages rajeunis de Marine Le Pen et celui de sa nièce de Reconquête, Marion Maréchal. Deux profils deepfakes qui faisaient la promotion de l'extrême droite en présentant une image glamour, jeune et moderne du parti grâce à de faux contenus générés par l'IA. Très bien faites, ces vidéos reprenaient les codes TikTok qui plaisent à la jeune génération[90] : des musiques tendances, accompagnées de chorégraphies réalisées par des jeunes filles, bien souvent sur fond de paysages clinquants. Le tout en mettant en avant leur plastique avantageuse et accompagné de commentaire de type : « *Quand le RN sera élu* », « *Moi quand je vais voter Reconquête en juin* », « *La robe que je vais porter pour la victoire de Jordan (Bardella)* » … Si l'on peut croire à de simples comptes parodiques créés pour faire sourire les internautes, ils semblent bien avoir été créés pour les tromper et faire la publicité du Rassemblement national auprès des jeunes utilisateurs. On pouvait même leur verser de l'argent. Les deux femmes politiques parodiées ont réfuté tout lien avec ces comptes. Car il est difficile de faire des liens entre ce genre de comptes et les campagnes de partis. Voilà une utilisation des deepfakes dans une campagne qui est simple, bon marché mais à l'efficacité difficilement quantifiable, mis à part les trente mille abonnés chacune[91].

Plus troublant, « *En Slovaquie, en mars 2024, une fausse conversation générée par IA mettait en scène la journaliste Monika Tódová et le dirigeant du parti progressiste slovaque Michal Semecka fomentant une fraude électorale. Les enregistrements diffusés sur les réseaux sociaux pourraient avoir influencé le résultat de l'élection. Le même mois, en Angleterre, une soi-disant fuite sur X fait entendre Keir Starmer, le leader de l'opposition travailliste, insultant des membres de son équipe. Et ce, le jour même de l'ouverture de la conférence de son parti. Un hypertrucage vu plus d'un million de fois en ligne en quelques jours* »[92].

Certains gouvernements sont moins regardant

Dans nos démocraties, le sujet des deepfakes est relativement bien pris au sérieux, que ce soit par nos politiques ou nos journalistes. Les alertes sont régulièrement lancées quand des photos ou des vidéos truquées sont mises en ligne. En revanche, certains gouvernements sont moins regardants.

Exemple avec cette utilisation beaucoup plus dérangeante, celle du pouvoir en place au Vénézuela. L'équipe du président Maduro en use et abuse. Les Vénézuéliens ont ainsi pu profiter de deux avatars, pseudo présentateurs de journal télévisé, vantant le renouveau de l'économie du pays. Une vision idéalisée du programme présidentiel pour contrer les déclarations des autres médias. « *Les présentateurs de House of News, Noah et Daren, ont été sélectionné parmi plus d'une centaine de visages multiethniques disponibles sur le software Synthesia … Mais ce vaste catalogue humain ne propose pas uniquement des journalistes comme Noah et Daren. On peut choisir un Dave avec un look de médecin ou de cadre supérieur, un Carlo avec des vêtements de travail et un casque et même le père Noël* »[93]. La propagande chez un dictateur n'est pas neuve, dans les années 1970 et 1980 les JT sur l'OZRT, l'Office Zaïrois de Radio-Télévision, étaient tout à la gloire du Maréchal Mobutu. Mais leur modernisation est bluffante, elles peuvent être adaptées et améliorées, et on peut les multiplier à l'envi pour discréditer le travail des journalistes, cibles très à la mode. Cela a permis également de montrer aux Vénézuéliens de faux JT étrangers, notamment américains et donc largement hostiles à Maduro, parlant positivement de leur pays, deepfakes à l'appui[94]. De quoi ajouter de la confusion à la confusion.

En Turquie, les élections présidentielles de mai 2023 ont été entachées par des deepfakes. Un candidat de l'opposition, Muharrem Ince, s'est ainsi retiré après avoir été la cible d'une campagne de dénigrement en ligne, qui comprenait notamment des images truquées de lui avec des femmes ou au volant de voitures de luxe. Plus étonnant encore, en plein meeting, Recep Tayyip Erdogan a diffusé un clip de quatorze secondes, présenté comme la preuve que son principal rival, Kemal Kiliçdaroglu, « *avance main dans la main avec le groupe armé PKK* »[95]. Kemal Kilicdaroglu, principal rival du président, a ensuite affirmé que des pirates étrangers, recrutés par le camp Erdogan, préparaient des deepfakes, vidéos ou sons manipulés grâce à l'intelligence artificielle, afin de le discréditer, ciblant principalement la Russie. Autre exemple, en 2024, le président turc Recep Tayyip Erdogan menait « *une bataille pour reprendre le contrôle d'Istanbul lors d'élections locales très disputées … Mais alors que le parti AK d'Erdogan intensifie ses efforts pour reprendre le contrôle de Istanbul, une vidéo générée par l'intelligence artificielle du maire sortant Ekrem Imamoglu félicitant Erdogan pour ses réalisations à Istanbul, a circulé sur les médias sociaux … Les médias indépendants ont alors mis en garde contre la menace de fausses nouvelles, car les médias traditionnels, qui sont principalement sous le contrôle du gouvernement*[96]*, ne vérifiaient pas l'authenticité des vidéos* »[97]. Le secteur des médias indépendants ferait face à une pression des autorités turques et une grande partie de leurs nouvelles seraient bloquées sur les médias sociaux. Une tendance confirmée par Emma Sinclair-Webb, chercheuse principale en Turquie de Human Rights Watch : « *Ce que nous avons vu, c'est que très, très souvent du matériel, principalement des nouvelles sur les médias sociaux, est supprimé et bloqué en ligne … Il est très inquiétant de voir que les autorités sont prêtes à réprimer la liberté d'expression, mais les entreprises de médias sociaux elles-mêmes ne sont pas assez robustes pour résister à cette pression* »[98]. La Turquie est ainsi un bon exemple de guerre de récits, en période électorale,

appuyé par des deepfakes. Mais ces derniers ne montrent une efficacité que grâce aux pressions gouvernementales sur les médias de presse et les médias sociaux. La pression sur ces derniers est bien réelle. Exemple avec le blocage en 2023 par Elon Musk de quatre comptes sur X, car il était effrayé par la menace du régime de bloquer son réseau social dans tout le pays. Car Erdogan ne plaisante pas et l'a montré en 2024, quand Instagram, pourtant utilisé par cinquante-sept millions de Turcs, a été complètement bloqué par les autorités qui n'ont pas donné de raison claire mais le président avait accusé le réseau social de censurer les critiques contre Israël et certains messages de soutien aux Palestiniens. Il a été jusqu'à parler de « fascisme numérique ». Voilà donc un exemple de pays qui montre combien la censure de deepfakes par les plateformes n'est pas la panacée, ces dernières n'étant pas en mesure de tenir tête à un régime autoritaire, à la tête d'un juteux marché de quatre-vingts millions d'âmes.

De plus, l'efficacité de deepfakes dépend beaucoup des contextes politiques locaux. En 2023, au Bangladesh, pays en proie à de vastes émeutes contre le régime, des dizaines d'experts, de spécialistes et autres écrivains ont été créés par l'IA pour défendre le bilan du gouvernement ou accuser des pays étrangers d'être responsables des problèmes économiques du pays. Faux articles, fausses photos. Le tout propagé par des médias nationaux. Peine perdue, la Première ministre Sheikh Hasina devra démissionner[99]. Il faut dire que cette autocrate était au pouvoir depuis quinze ans et que, quel qu'ait pu être sa communication, il était trop tard pour convaincre un peuple écœuré et révolté.

Comme le précise Danielle Citron, spécialiste des deepfakes et professeure à la Faculté de droit de l'Université de Virginie : « *La possibilité d'influencer le résultat d'une élection est réelle, en particulier si l'auteur est capable de programmer la diffusion de manière à ce qu'il y ait suffisamment de temps pour que le contenu trafiqué circule, mais pas assez pour que la victime puisse le démentir efficacement – à supposer qu'il puisse être démenti* »[100]. L'efficacité politique d'un deepfake dépend donc non seulement du contexte politique mais aussi du timing de sa publication et sans doute de la manière dont il est diffusé. L'Inde est ainsi un laboratoire pour les deepfakes publiés en période électorale. Dans cet immense pays, où la désinformation est largement utilisée, et où une grande partie de la population est peu éduquée aux subtilités des médias numériques, on a pu voir « *Des hommes politiques défunts ressuscités pour soutenir un candidat dans le Tamil Nadu ; un dirigeant d'un parti musulman entonnant des chants de dévotion hindous ; des stars de Bollywood d'habitude très discrètes, Ranveer Singh et Aamir Khan, critiquant ouvertement le premier ministre indien et apportant leur soutien au Congrès, le principal parti d'opposition… Les deepfakes (ou hypertrucages), ces vidéos reproduisant à s'y méprendre visages et voix et pouvant servir à propager de la désinformation, ont envahi les réseaux sociaux, comme les fake news avaient déjà marqué la campagne de 2019* »[101]. Plus efficace encore, un message vocal personnalisé du président nationaliste Narendra Modi adressé à chaque électeur en l'appelant par son nom, via WhatsApp. L'avatar du président leur parle des avantages gouvernementaux qu'ils ont reçus et demande leur vote. Le tout réalisé par l'équipe de communication du président, sans que ce dernier n'ait à y travailler une seconde. C'est une nouvelle méthode pour parler directement aux électeurs via des *chatbots* élaborés, qui leurs fait croire qu'il les connaît et connaît leurs problèmes. Pour Suhasini Raj, qui a écrit un article sur ces méthodes pour *The New-York Times*, « *Pour avoir un aperçu de l'avenir de l'intelligence artificielle dans les campagnes électorales, regardez ce qu'il se passe en Inde* »[102]. Car M. Modi n'est pas le seul à utiliser ce système qui pourrait faire des émules dans d'autres pays. La méthode, qui rappelle celle de Cambridge Analytica aux USA et en Grande-Bretagne en 2016, pourrait amener à la propagation de mensonges et de désinformations personnalisés juste pour gagner une élection. Pour Nicolas Obin, Maître de conférences à Sorbonne Université et chercheur à l'Ircam (Institut de recherche et coordination acoustique/musique), il existe des manipulations pernicieuses, « *comme la manipulation des émotions, qui s'adresse à nos affects. Par exemple, un assistant vocal pourrait avoir des interactions émotionnelles ou expressives et influencer nos comportements en infléchissant nos émotions, ou en nous incitant à acheter quelque chose, etc. En politique, un même discours pourrait être adressé à chaque citoyen avec des variations de ton adapté pour obtenir un effet optimal de persuasion* »[103]. Là on entrerait dans la manipulation caractérisée.

La propagation de mensonges et de désinformations personnalisés

En février 2022, le candidat conservateur sud-coréen, Yoon Suk-Yeol, présentait son avatar, histoire d'attirer les jeunes, lassés par les politiciens qu'ils estimaient trop éloignés de leurs problèmes. Cet avatar, un deepfake, répondait aux questions des citoyens sur le net avec un langage humoristique et satirique, utilisé dans les jeux en ligne, avec des phrases calibrées[104] pour devenir virales. Exemple : « *Le président Moon Jae-in et Lee Jae-myung (le candidat du parti au pouvoir, ndlr) se noient. Lequel sauvez-vous?* », demande un internaute, « *Je leur souhaite bonne chance à tous les deux* » rétorque l'avatar. Des répliques faites pour devenir virales, en réalité données par une équipe de campagne et non par le candidat lui-même. Les adversaires ont eu beau reprocher au candidat de rabaisser le niveau de la campagne, des millions de questions ont été posées dans ce pays qui compte l'Internet le plus rapide du monde. Dans une interview, le directeur de la campagne de l'avatar, Baik Kyeong-hoon a déclaré : « *Les mots prononcés le plus souvent par Yoon sont mieux reproduits dans l'avatar* » et « *Il est inévitable*

que cette technologie soit utilisée dans de futures élections »[105].

Et encore une fois, Internet aura été au centre d'une élection présidentielle, puisque le 10 mars dernier, Yoon Suk-yeol s'impose dans le scrutin le plus serré de l'histoire de la Corée du Sud. Avec une carrière politique éclair, un programme conservateur et une personnalité controversée, il est parfois surnommé le « Donald Trump coréen » ou K-Trump[106]. Même si le gendarme électoral de Corée du Sud autorise les avatars de candidats à condition qu'ils soient identifiés comme technologie deepfake et ne diffusent pas de la désinformation, on peut encore une fois se demander, comme pour les candidats en Inde, si on ne donne pas l'illusion aux citoyens que c'est le candidat qui répond directement à leurs questions avec un langage qui n'est pas du tout le sien ? N'est-ce pas une fausse impression de proximité avec le candidat ? D'autant qu'il est qualifié de piètre orateur et surnommé « Monsieur une gaffe par jour ». Cela ouvre un autre débat : une personnalité politique doit-elle avoir du charisme et être bonne oratrice pour diriger un pays, et les deepfakes ne sont-ils pas une solution à ce problème ? Nul doute que ces questions risquent de revenir à l'avant plan dans divers pays du monde.

Il est clair que la guerre de l'information est l'une des composantes de la guerre et, dans un contexte géopolitique international en pleine restructuration où les grandes nations comme la Chine, les États-Unis, l'Iran ou encore la Russie peuvent ne pas se faire de cadeaux, à quels types de vidéos doit-on s'attendre pour discréditer l'adversaire ? Rappelons-nous comme Chine, Russie et États-Unis se sont livrés à une bataille de propagandes acharnées quant à la responsabilité de l'un ou de l'autre face à la pandémie de Covid-19.

En 2022, les Ukrainiens, en pleine guerre, ont pu entendre et voir un deepfake de leur président annonçant « *Je vous recommande de déposer les armes et de retourner auprès de vos familles. Vous ne devriez pas mourir dans cette guerre. Je vous demande de vivre, et je compte faire de même !* »[107]. Le site de la chaîne nationale Ukraine 24 avait été piraté et relayait la vidéo, comme pour lui donner plus de crédit. Mais le gouvernement avait préalablement et largement prévenu son armée de ce genre de risque et des alertes au fake ont rapidement été lancées par la chaîne nationale et par Meta. Il faut également ajouter que le deepfake n'était, étonnement, pas d'une grande qualité.

Ajoutons qu'un deepfake n'est pas souvent nécessaire pour convaincre. Souvenons-nous qu'avant l'invention de l'hypertrucage, des photos satellites de prétendues armes de destruction massive, avaient été présentées par les États-Unis devant le Conseil de Sécurité de l'ONU le 5 février 2003, afin de discréditer au maximum le régime de Saddam Hussein et de légitimer une attaque de l'Irak. On sait que tout cela était faux.

Politiquement, les deepfakes n'ont pas encore prouvé qu'ils étaient d'une efficacité considérable, comme beaucoup le craignent depuis plusieurs années. Ils sont un outil supplémentaire de propagande et de désinformation parmi des milliers d'autres, mais ils sont aussi très visuels et cela ajoute à la confusion. Antonin Descampe, professeur en journalisme et en innovation média à l'UCLouvain, parle carrément de « désordre informationnel massif » plutôt que de désinformation. « *On se retrouve aujourd'hui dans une situation dans laquelle effectivement tout contenu, qu'il s'agisse de texte mais également d'audio, de vidéo, d'image, peut potentiellement avoir été généré, éventuellement partiellement, par une intelligence artificielle. Et donc on se retrouve dans une situation où le citoyen est dans un état de confusion. Il ne sait pas si la photo a été prise véritablement ou fabriquée par une intelligence artificielle, et cela ne lui permet pas de faire des choix éclairés dans son environnement* »[108]. Il est actuellement impossible de connaître l'impact de toutes ces fausses informations mais on sait qu'elles peuvent influencer un jugement, comme démontré par Olivier Klein, professeur de psychologie sociale à l'ULB. Selon son étude, « *Même une information que l'on sait fausse nous influencera* »[109].

En revanche, ce qui nous semble être un danger provoqué par des deepfakes, c'est l'avenir de la preuve vidéo, audio ou autre, qui peut être présentée comme fausse. Ce fut déjà le cas en Afrique centrale fin 2018. Le président gabonais, Ali Bongo Ondimba, se faisait soigner à l'étranger depuis plusieurs semaines suite à un AVC. Son discours à la nation, prononcé le 31 décembre 2018, devait rassurer la population inquiète et faire taire toute rumeur de décès. Mais celle-ci fut accusée d'être un deepfake, par ses opposants politiques, et a servi de déclencheur, une semaine plus tard, à un coup d'État infructueux de l'armée gabonaise, à Libreville, le 7 janvier 2019. La première tentative de coup d'État au Gabon depuis 1964[110].

En 2018, Joao Doria, le gouverneur de Sao Paulo au Brésil, marié, a affirmé qu'une vidéo qui le montrait lors d'une orgie sexuelle était un faux et personne n'a pu prouver de manière concluante que ce n'était pas le cas.

Les deepfakes posent ainsi une question très importante : pourrait-on désormais discréditer toute preuve de malversation politique, qu'elles soient vidéos, audios, scripturales ou autre ? Un commentaire déplacé d'un chef d'état comme Trump lui suffirait pour invoquer un deepfake, comme il a qualifié de fake news tout ce qui desservait sa cause[111]. Autre cas de figure, en mai 2019 le chancelier conservateur autrichien Sebastian Kurz avait annoncé la démission de l'ensemble des ministres d'extrême droite, à la

suite de la diffusion d'une vidéo compromettante pour le FPÖ. On y voyait, en caméra cachée, le chef du FPÖ, Heinz-Christian Strache, se dire prêt à accepter des financements russes occultes[112]. Cet Ibizagate, comme on l'a surnommé, confirme, d'une part, combien les mandats ministériels restent fragiles face à une vidéo compromettante, mais on peut désormais aussi se demander s'il sera encore possible à l'avenir d'utiliser comme preuve une telle vidéo vu l'accessibilité croissante aux technologies du deepfake.

Pourra-t-on désormais croire une image de caméra de surveillance souvent de moindre qualité ? Ou celle d'un témoin de violences impliquant une personnalité ou un agent de l'état ?

02. Propagandes 4.0.

Nous l'avons vu, des manipulations de l'opinion par les gouvernements sont également envisageables, notamment depuis l'étranger. Si la Russie a clairement tenté d'influencer les élections américaines en 2016, d'autres de ses méthodes sont moins connues. Ainsi, un rapport[113] d'experts français souligne combien des continents comme l'Afrique ou l'Amérique latine, avec des langues communes à plusieurs pays et des populations moins averties – et néanmoins très connectées grâce à la démocratisation des technologies de l'information et de la communication – étaient susceptibles d'être traversées de passions faciles à instrumentaliser, dont des tensions ethniques et religieuses, et un ressentiment à l'égard des anciennes puissances coloniales. Le rapport cite le cas du Maghreb, où les populations sont largement exposées à la propagande des médias russes en arabe, qui véhicule des messages anti-européens, dont elles ne sont que la cible indirecte, le vecteur. L'objectif est que ces populations, qui sont en lien quotidien avec leurs familles et leurs proches vivant en Europe, leur transmettent ces messages et les convainquent que les médias européens leur mentent et que les Européens leur sont hostiles. La propagande anti-immigration que l'on voit en Europe visant à exciter les communautés nationalistes n'est donc qu'une face de l'opération. Pour diviser, monter les communautés les unes contre les autres, il faut aussi convaincre les populations issues de l'immigration qu'elles sont maltraitées et, de ce point de vue, le fait de passer par des relais en Afrique du Nord est particulièrement habile[114]. Et pour sa propagande, la Russie n'hésite pas à utiliser des deepfakes. On peut citer l'exemple d'une vidéo de JT de France 24, annonçant qu'Emmanuel Macron aurait annulé sa visite en Ukraine en raison d'un projet d'assassinat contre lui en Ukraine[115]. Il est à noter que les journalistes souvent traités de menteurs sont régulièrement utilisés comme sources fiables par les complotistes pour créditer leurs théories.

Beaucoup craignent ainsi que les deepfakes ne s'ajoutent à des manipulations d'opinion, à l'attisement de réactions émotionnelles, à la création de scandales politiques pour affaiblir un gouvernement, voire même à des dissensions entre deux États en les cumulant à des cyberattaques.

03. La tentation des "campagnes positives"

Un article du *Vice Magazine*[116] soulève un aspect inquiétant d'une campagne électorale en Inde. Le 7 février 2020, un jour avant les élections à l'Assemblée législative à Delhi, le président du Parti Bharatiya Janata (BJP), Manoj Tiwari, critique face caméra le bilan de son adversaire politique dans trois vidéos identiques mais chacune dans une langue différente : hindi, anglais et haryanvi, un dialecte du nord de l'Inde. Mais seule la première a été réellement prononcée par le candidat, les autres sont des deepfakes. L'un des objectifs de l'homme politique était bien sûr de cibler particulièrement les électeurs migrants venant d'Haryana et qui travaillent à Dehli pour les convaincre de ne pas voter pour le ministre en chef sortant[117].

Normaliser ces "deepfakes positifs" pourrait ouvrir une boîte de pandore

« *La technologie Deepfake nous a aidé à intensifier les efforts de campagne comme jamais auparavant* », a déclaré le co-responsable des médias sociaux et de l'informatique pour BJP Delhi. Selon lui, quinze millions de personnes ont vu ces vidéos diffusées via des milliers de groupes WhatsApp, application ultra populaire en Inde. Bien sûr l'intention est de se faire comprendre d'un maximum de gens, en évitant les sous-titres qui n'auraient pu être lus par une partie analphabète de la population, mais cela reste faux et laisse à penser que ce candidat, parlant l'haryana, est des leurs et les comprend dès lors mieux qu'un autre qui ne parle pas cette langue. Un deepfake, même avec le consentement de la personne et de bonnes intentions, reste un faux. Il doit donc être assumé, ou à tout le moins, signalé.

D'un côté, normaliser ces « deepfakes positifs » pourrait ouvrir une boîte de pandore car l'IA permet des traductions désormais quasi simultanées, et promet de banaliser le phénomène, mais peut aussi faire parler un avatar aux électeurs. Jusqu'où peut-on utiliser cette technologie pour montrer une belle image d'un candidat ou conforter une idéologie ? Désormais, on voit par exemple, des fans de Trump créer leur propre réalité, notamment avec des photos « hypertruquées » de leur candidat préféré aux côté de nombreux Noirs-Américains, des avatars créés par l'IA, comme pour convaincre qu'il n'est pas si suprématiste qu'on le prétend. Alors que devoir créer une telle photo, n'est-ce pas démontrer qu'il n'en existe pas de réelles ?

118

Gageons que les citoyen·ne·s du monde entier aient le temps d'être mis au courant de l'existence de ces nouvelles possibilités technologiques qui jouent sur notre perception du monde.

04.Faux témoignages idéologiques

On pourrait imaginer des personnages, créés de toute pièce, faire de faux témoignages. Quels seraient les réactions à chaud du public dans une situation de crise par exemple ?

Citons l'exemple de Jenna Adams qui, de 2014 à 2017, « était une militante pro-Trump connue », icône de l'alt-right américaine[119], citée par les grands médias (dont *The Washington Post*, *The New York Times*, *The Independent* et France 24) et suivie par septante mille comptes sur Twitter. Mais Jenna Abrams n'existait pas : son compte était une création de l'IRA, usine à trolls basée à Saint-Pétersbourg. L'intelligence artificielle rendra ces personnalités fictives plus sophistiquées, moins détectables. Elles pourront donner des interviews en visio-conférence, écrire des tribunes dans la presse, avant d'être découvertes.

Autre cas incroyable, celui d'au moins dix-neuf faux journalistes ou faux experts en géopolitiques qui ont été publiés dans de nombreux journaux anglophones conservateurs. Leurs articles et éditos faisaient l'éloge des Émirats arabes unis et dénonçaient la politique du Qatar, se montrant sceptiques envers la politique de Facebook. Et tous ces pseudo-spécialistes… n'existaient tout simplement pas. Les usurpateurs récupéraient par exemple la photo d'un véritable humain et la modifiaient de manière à ne pas pouvoir être retrouvés avec une recherche inversée. Dans certains cas, les photos de profils montraient des personnes créées par intelligence artificielle. En plus de cette fausse identité ils s'étaient fait un faux CV sur LinkedIn et ils étaient, pour la majorité, des contributeurs sur deux sites construits de toutes pièces : The Arab Eye et Persia Now. Certains articles ont même été relayés par des personnalités comme Ryan Fournier, le cofondateur de l'association Students for Trump, et suivi par près d'un million de personnes sur Twitter, ou encore la sénatrice française de l'Orne, Nathalie Goulet. L'IA va énormément faciliter et diversifier la fabrication de ces pseudo preuves d'existence d'experts, de journalistes, de témoins…

Les hypertrucages risquent ainsi de donner de nouvelles idées de faux témoignages aux *trollers* et aux partisans et idéologues de tout poil.

05.Huile sur le feu

En avril 2015, la police de Baltimore arrête et embarque violemment le jeune afro-américain Freddie Gray qui mourra de ses blessures une semaine plus tard. Sa mort conduira aux émeutes de Baltimore de 2015. Sans parler de Georges Floyd et de Jacob Blake en 2020 et des autres cas de violences policières abusives, voire mortelles, à caractère raciste.

Dans ce genre de climat de haute tension entre communautés, que se passerait-il si une vidéo trafiquée d'un policier tenant des propos racistes par exemple était lancée sur les réseaux sociaux ?

Les manifestations des gilets jaunes ont été un vivier de fake news. De tout temps les fausses informations ont attisé des émeutes voire des révolutions à l'instar de la fameuse phrase apocryphe de la reine de France Marie-Antoinette parlant du peuple : « *Ils n'ont pas de pain ? Eh bien qu'ils achètent de la brioche* » juste avant la Révolution française. Un deepfake risque ainsi d'être un catalyseur de violences en pleine tension sociale ? Et si les pouvoirs en place venaient à souligner qu'une vidéo est fausse, seraient-ils seulement cru par les manifestants ?

D'un point de vue politique, les partis extrémistes ont montré qu'ils étaient capables de mettre de l'huile sur le feu pour appuyer leurs thèses. Il suffit qu'un migrant commette un crime pour que toute la communauté, particulièrement africaine et/ou musulmane, soit mise dans le même sac. Exagération, manipulation, décontextualisation ont déjà été largement utilisés par ceux-ci. La correspondante pour France 24 en Italie écrivait quelques semaines avant les élections européennes de 2019 : « *En Italie, les "fake news" ont eu davantage de visibilité que les "vraies" informations selon l'autorité de régulation de l'information (AGCOM)* »[120].

Soulignant l'exemple de cette vidéo montrant soi-disant des migrants en train de vandaliser une voiture de carabiniers qui a été vue près de dix millions de fois sur une page de soutien au leader de la Ligue Matteo Salvini. Il s'agissait en fait d'un extrait de film de fiction. Les deepfakes risquent ainsi d'amener encore plus de confusion à une confusion politique, voire envenimer une tension sociale.

06. Galéjades en cascade pour noyer le poisson

Autre danger : « *l'altération discrète d'une partie seulement d'un contenu audio ou vidéo, un discours par exemple. Ou encore la possibilité d'en faire un grand nombre de variations - diffuser une vingtaine de variantes du même discours, par exemple, pour diluer l'authentique dans la confusion* »[121]. Multiplier les faux pour noyer le vrai. Des deepfakes peuvent en effet être créés à l'envi. À la diffusion d'une vidéo compromettante pour une personnalité X, il serait facile d'en créer une autre en prétendant que celle-là est la vraie. Les adeptes de M. ou Mme X seraient tentés d'en produire même plusieurs pour transformer l'originale en faux parmi tant d'autres, accentué par l'effet polarisant des réseaux sociaux qui voit souvent s'affronter les pour et les contre. De quoi en perdre son décryptage.

En 2004, en pleine campagne présidentielle entre le démocrate John Kerry et Georges W. Bush, une « *photographie, faussement attribuée à Associated Press, combinait deux images distinctes pour donner l'impression que M. Kerry partageait une scène lors d'un rassemblement anti-guerre au début des années 1970 avec l'actrice, Jane Fonda* »[122]. Le but était de discréditer Kerry, ancien vétéran du Vietnam, en le mettant en présence d'une comédienne considérée comme traîtresse à la patrie après son voyage de 1972 à Hanoï, la capitale de la République démocratique du Viêt Nam d'Hô Chi Minh. Il est intéressant de constater ici que d'une part les trucages font partie des campagnes depuis longtemps, même dans les pays démocratiques, et que d'autre part, différents opposants à Kerry, ont affirmé que l'image originale avait été fabriquée et que c'était l'image combinée qui était l'image réelle avant que ne soit officiellement démontré le trucage.

Un ou plusieurs deepfakes pourraient ainsi jeter le discrédit sur une vraie info et une vraie information.

07. Du flou pour les géants du Net

Beaucoup de gouvernement incitent les GAFAM à réguler les deepfakes, les audios et vidéos mensongers. Mais comment concilier les points de vue ? Car certaines décisions sont inévitablement politiques. Ce qui est acceptable aux États-Unis, ne l'est pas forcément en UE ou aux Philippines. D'autant que s'il y a un paquet d'argent à la clé, on trouvera toujours un endroit pour produire des deepfakes. Citons quelques exemples pour percevoir la complexité des choix à effectuer par les plateformes.

Rien qu'aux États-Unis, les GAFAM ont régulièrement des choix « *politiques* » à faire. Traditionnellement depuis le début de notre siècle, les Républicains reprochent aux patrons du numérique d'être plutôt démocrates. Juillet 2022, le service de vidéos de Google, YouTube, a « *ajouté les contenus sur l'avortement à ses règlements sur la désinformation médicale, qui interdisent déjà les contenus faux ou trompeurs sur la COVID-19 ou les vaccins. Par exemple, "les affirmations selon lesquelles les avortements sont très risqués ou causent souvent des infertilités ou des cancers", précise le groupe californien … Les plateformes craignent en effet que les informations personnelles de femmes qui ont avorté ou d'individus qui les auraient aidées (recherches en ligne, déplacements en Uber, etc.) ne soient retenues contre eux par les procureurs d'États conservateurs ayant interdit l'avortement* »[123]. Des informations de santé publique qui sont apparues comme ouvertement démocrates aux yeux de nombreux conservateurs.

À l'été 2022, Facebook a fait l'objet de vives critiques, aux États-Unis, pour avoir « *communiqué à la justice le contenu de conversations entre une mère et sa fille de 17 ans dans un dossier d'avortement illégal* »[124]. Face à la justice, les GAFAM ne peuvent garantir l'anonymat de leurs abonnés, qui peuvent devenir hors la loi suite à une décision de la Cour suprême.

Comment réguler universellement les différentes thématiques ? Difficile pour les amateurs d'art d'accepter la censure d'œuvres d'art, comme la fameuse *Origine du monde* de Courbet, sous des prétextes de pudeur voire de pudibonderie[125].

Ou que faire quand un Donald Trump, alors président des États-Unis, publiait jusqu'à vingt-deux mensonges par jour, à une période de son mandat, selon le *Washington Post*, journal plutôt critique à l'égard de Trump en général ? Le président a été censuré puis exclu du réseau. Non seulement il a créé son propre réseau social de microblogage, du Trump Media & Technology Group (TMTG), mais cet acte a suscité nombre de critiques au pays de la liberté d'expression. Le résultat a été le rachat de Twitter par Elon Musk et la réhabilitation de Trump sur le réseau, qui est également devenu entre-temps, comme souligné dans la publication *Les dangers démocratiques du numérique*, le lieu d'expression de l'extrême-droite. 2024 semble être l'année de la question : « comment mettre au pas des réseaux sociaux à la puissance démesurée et utilisés par la majorité des citoyens ? ».

Un deepfake est un faux me direz-vous, il suffit de l'indiquer. Mais cette notion est toute relative. Penser qu'il ne peut exister qu'un point de vue à l'échelle de la planète, et sur tous les sujets, afin de légiférer, semble presque illusoire. Et puis nombre de deepfakes, risquent d'être présentés comme de la satire, ce qu'un juge devra apprécier. Oui mais un juge de quel pays ?

Nous le verrons, la plupart des réseaux sociaux y travaillent, même si d'autres beaucoup moins, comme X ou Telegram.

Le débat sur la censure du fake est loin d'être résolu, d'autant qu'affiner les décisions des algorithmes prend du temps et que ceux-ci sont, en grande majorité, programmés aux États-Unis et en Chine, deux pays qui n'ont pas exactement les mêmes valeurs démocratiques que la Belgique, notamment sur le respect de certaines minorités ou des personnes précarisées. La mathématicienne américaine Cathy O'Neil met en garde contre « *les dangers de certains algorithmes, aux impacts destructeurs dans la justice, l'éducation, l'accès à l'emploi ou au crédit* »[126]. Les algorithmes reproduisent les inégalités sociales et leur programmation reste trop opaque pour le monde entier[127]. Un algorithme n'a aucune conscience des inégalités qu'il porte en lui, alors comment va-t-il estimer un message à tendance raciste, sexiste ou en défaveur des précarisés ?

Discussions et bras de fer font évoluer les débats, entre acteurs et décideurs, mais la technologie évolue bien trop et, désormais, on assiste à une course à l'IA planétaire et phénoménale, qui rend une régulation encore plus urgente mais encore plus complexe.

4. Je ne crois que ce que je vois, enfin je crois

Selon Nicolas Obin : « *Par leur ultra-réalisme, il devient de plus en plus difficile voire impossible de distinguer un vrai d'un faux. Il peut cependant subsister des indices, comme par exemple des déformations ou des incohérences de synchronisation labiale ou entre les expressions du visage. Mais elles sont de plus en plus subtiles. Néanmoins, toute manipulation laisse une trace caractéristique, même imperceptible par un être humain. La détection de ces traces par des IA nécessite de les retrouver et de les identifier. Le problème est qu'il existe une grande variété d'algorithmes de génération, ce qui augmente considérablement la complexité pour les identifier. Et comme l'algorithme utilisé pour la génération est inconnu lorsque nous devons essayer d'identifier un deepfake, il devient extrêmement difficile de proposer une solution universelle de détection robuste à toutes les formes d'attaques* »[128].

Diverses personnalités politiques misent encore sur les initiatives visant à renforcer l'éducation aux médias pour cultiver un public averti. Mais il nous semble quelque peu illusoire d'espérer que l'éducation aux médias arrive à suivre, par exemple, les évolutions de l'IA qui s'affinent chaque jour et des possibilités multiples qu'elle offrira bientôt. Sans parler des inconnues sur son fonctionnement, qui reste flou même pour les experts. Autant demander aux mêmes politiques d'adapter leurs lois à cette vitesse.

En Éducation permanente, nous tentons d'informer, d'éveiller aux multiples dangers d'Internet, mais les différents publics sont loin de se passionner pour le fonctionnement du Net, pour la logique des datas ou tout simplement pour un cookie. Rien que la technique de l'image inversée, qui permet de recontextualiser l'origine d'une photo, est excessivement peu utilisée. Dans un *skrolling* où chacun fait défiler les images à des rythmes effrénés, demander de vérifier tout ce qu'on voit est absurde. Les personnes voient une image, l'apprécient ou non, la partagent ou non, le tout prend une demi-seconde. La plupart du temps ils n'ont cure de leur véracité. Ce qu'ils cherchent c'est de l'émotion, comme le joueur devant un bandit-manchot attend de voir des pièces tomber pour vibrer quelques instants.

De plus en plus de spécialistes nous disent que la sophistication des avancées technologiques est telle, qu'imaginer que tout citoyen puisse distinguer les vraies images des fausses est illusoire. Sam Gregory, directeur exécutif de WITNESS, une organisation internationale à but non lucratif qui aide le public à utiliser la vidéo et les technologies pour protéger et défendre les droits de l'homme, explique ainsi que « *Les conseils qui consistent à "repérer les mains à six doigts", à inspecter les erreurs visuelles sur l'image du Pape en doudoune, à vérifier si une image suspecte cligne des yeux ou à écouter très attentivement le son dans l'espoir d'entendre une erreur ne sont pas suffisants et ne sont d'aucune utilité à long terme, ni même à moyen terme … C'est pourquoi il est urgent de mettre en place une législation ciblée, des techniques dynamiques relatives à la provenance et à la divulgation, ainsi que des outils de détection des dommages potentiels, afin de faire face aux menaces croissantes. Ces mesures doivent s'accompagner d'efforts de collaboration de la part de l'industrie des technologies, de la société civile et des décideurs politiques. Comme toujours, les parlements joueront un rôle essentiel pour mettre tous les acteurs sur la même longueur d'onde* »[129]. En 2023, la RTBF a proposé un jeu où il fallait dire, parmi vingt photos, si elles avaient été générées par l'IA ou non. Sur les cinq ou six personnes qui l'ont testé au bureau, aucun n'a fait plus que 16/20, malgré une concentration bien plus appuyée que lors d'un scrolling sur Instagram[130].

5. Des chiffres alarmants et des responsables alarmés

Depuis les ingérences russes dans les élections américaines de 2016, le monde plonge inexorablement dans l'ère de la cyberguerre[131]. Et le Pentagone, comme l'UE, se montrent très inquiets face aux deepfakes alors même que les opérations militaires se digitalisent aussi[132]. Le Colonel américain Liam Collins citait ainsi diverses techniques modernes de guerre de l'information opérées par les Russes. Par exemple des attaques personnalisées envers des militaires en opération, comme ce fut le cas en Ukraine, déjà en 2015, où le Kremlin envoyait des SMS aux soldats ukrainiens *« visant à altérer leur moral ou leur cohésion, leur signifiant par exemple qu'ils étaient "encerclés et abandonnés". Puis, quelques minutes plus tard, leurs familles recevaient un message leur annonçant la mort de leur fils, leur frère ou leur père, tué par l'ennemi - ce qui suscitait généralement des appels des familles vers les soldats, et permettait, par la concentration de signaux, de détecter leur localisation pour ensuite les bombarder »*[133]. Au vu de ce type de technique, on pourrait se demander comment un soldat réagirait sur le terrain à une vidéo truquée de sa famille ou répondrait à un faux ordre donné par un supérieur via un deepfake audio ou vidéo ? D'autant que l'armée se digitalise de plus en plus. Début 2019 déjà, *« Le directeur du Renseignement américain, Dan Coats, a déclaré devant le Congrès, s'attendre à ce que des puissances étrangères hostiles "militarisent des deepfakes" contre les États-Unis et leurs alliés, afin de semer chez eux le doute et la discorde »*[134]. L'agence de recherche du Pentagone, la Darpa, (Defense Advanced Research Projects Agency)[135], collabore avec plusieurs des plus grandes institutions de recherche des États-Unis afin de prendre de l'avance sur les dérives graves possibles. Exemple à l'Université du Colorado de Denver, où des chercheurs travaillent sur le programme de la DARPA pour créer des deepfakes convaincants. Ceux-ci seront ensuite utilisés par d'autres chercheurs qui développent des technologies pour détecter ce qui est réel et ce qui est faux[136]. Ce ping-pong entre chercheurs permet de suivre les évolutions technologiques et de tenter de devancer toute personne mal intentionnée.

Politiciens, journalistes et experts ne cessent de s'inquiéter du phénomène. En février 2024, des experts en intelligence artificielle, dont des sommités belges[137], et des patrons d'industrie ont signé une lettre ouverte[138] appelant à plus de réglementation autour de la création de deepfakes, citant les risques potentiels pour la société. La lettre a été rédigée par Andrew Critch, chercheur en IA à UC Berkeley. Nous allons en grande partie l'évoquer dans ce chapitre car elle illustre parfaitement les craintes et les propositions des experts de la question.

Selon eux, « *Les nouvelles lois devraient :*

- *complètement criminaliser la pornographie enfantine deepfake, même lorsque seuls des enfants fictifs sont représentés ;*
- *établir des sanctions pénales pour quiconque crée ou facilite sciemment la propagation de deepfakes nuisibles ;*
- *exiger des développeurs de logiciels et des distributeurs que leurs produits audio et visuels interdisent de créer des deepfakes nuisibles, et d'être tenus responsables si leurs mesures préventives sont trop facilement contournées.*

Si elles sont conçues à bon escient, ces lois pourraient nourrir des entreprises socialement responsables et n'auraient pas besoin d'être excessivement lourdes ».

En effet, tout va beaucoup trop vite. Demander à nos sociétés de fonctionner aussi rapidement que l'IA est une illusion et est peine perdue. Il faut absolument instaurer des garde-fous. Nous l'avons vu, aujourd'hui, les « deepfakes » concernent souvent l'imagerie sexuelle, la fraude ou la désinformation politique. Il y a urgence en ce qui concerne les deepporns, notamment la pédopornographie.

La lettre des experts fait référence à différentes études aux chiffres édifiants.

01. La pornographie, reine du deepfake

L'étude d'une association américaine d'experts en sécurité en ligne, SecurityHero[139], obtient des résultats interpellant. Morceaux choisis :

- Le nombre total de vidéos en ligne en 2023 est 95 820, représentant une augmentation de 550 % par rapport à 2019. Et rien qu'entre 2022 et 2023, la quantité de pornographie deepfake créée a augmenté de 464 %.
- La pornographie représente 98 % de toutes les vidéos deepfake en ligne.
- 99 % des personnes ciblées dans la pornographie deepfake sont des femmes. 58 % sont des chanteuses, 33% sont des actrices.
- Il faut désormais moins de vingt-cinq minutes et zéro euros pour créer une vidéo pornographique de soixante secondes de quiconque, en utilisant une seule image nette de son visage.
- 48 % des hommes américains interrogés ont vu de la pornographie deepfake au moins une fois. Et 74 % des utilisateurs de pornographie deepfake ne se sentent pas coupables à ce sujet. 20 % des participants à l'enquête ont envisagé d'apprendre à créer une pornographie deepfake.

- Sept des dix plus grands sites pornographiques hébergent des deepfakes.
- Parmi les dix plus gros sites Web dédiés à la pornographie deepfake, les vues vidéo cumulatives totalisent un nombre de 303 640 207.

Enfin, l'étude souligne deux facteurs importants qui ont joué un rôle central dans l'explosion des deepfakes : la montée en puissance des Réseaux Génératifs Adversaires (GAN) et la disponibilité croissante d'outils, de logiciels et de communautés pour leurs créations. Les outils et logiciels sont désormais accompagnés d'interfaces graphiques intuitives et plus accessibles. Le nombre d'outils conviviaux rendant la génération de contenu deepfake plus accessible est en augmentation, l'étude en a repéré pas moins de quarante-deux, destinés à un large éventail d'utilisateurs.

Autres chiffres instructifs : Les chanteurs et actrices sud-coréens constituent 53 % des personnes représentées dans la pornographie deepfake au monde. C'est le groupe le plus souvent ciblé. Suivent les États-Unis avec 20 %, le Japon : 10 %, l'Angleterre : 6 %, la Chine : 3 %, l'Inde : 2 %, Taïwan : 2 %, Israël : 1 %, Autres : 4 %. Cette diversité géographique souligne combien la prise de décision doit être globale et concertée.

Chez nous, le site deepfuck.com présente un choix de vedettes, au visage incrusté dans des scènes pornographiques. Il est spécialement dédié à ce genre de vidéos manipulées.

02. La cybercriminalité, un argent tellement facile

Autre étude intéressante, celle d'Onfido, une société de lutte contre la fraude qui remet un rapport sur la fraude en matière d'identité chaque année depuis 2019. Quelques éléments de celui de 2024[140] :

- 71 Millions de personnes sont victimes de cybercrimes globalement chaque année.
- 20% des Européens ont été victimes de vols d'identité de 2022 à 2024, sur la base des recherches de la Commission européenne.
- Un Américain sur trois a été victime de fraude d'identité.
- La fraude coûte à peu près six milliards de dollars de dommages-intérêts à l'économie mondiale, chaque année.

Cette étude montre l'explosion de l'utilisation des deepfakes dans la cybercriminalité. Et elle ne risque pas de s'arrêter là au vu des ce qu'elle rapporte. D'autant que jusqu'ici, on pouvait encore se rabattre sur la biométrie pour lutter contre la fraude, *« mais la facilité d'accès à l'IA générative et aux applications d'échange de visages a créé une nouvelle voie pour les fraudeurs ».*

03. Les élections

Nous avons déjà évoqué ce chapitre, notamment avec les faux coups de fil de Joe Biden, les deepfake sur Kamala Harris partagé par Elon Musk ou encore les exemples indiens, turcs ou bangladais. C'est également un aspect qui inquiète fortement les experts mais, à ce jour, ils n'ont pas encore démontré qu'ils pouvaient faire basculer une élection. Difficile pour nous-même de savoir parfois ce qui a influencé notre vote. Cela peut être la phrase d'un voisin, une info de presse, une image à la télé ou un deepfake. D'autant que les personnalités politiques sont très réactives lorsqu'il s'agit de dénoncer la diffusion d'un deepfake politique. C'est sans doute le type de fake news le plus surveillé au monde par ces derniers.

En revanche, ces outils utilisés par des dictateurs face à une population peu éduquée aux médias peut faire bien plus de dégâts. Idem dans des pays fracturés, comme le sont les États-Unis actuellement, où les deepfakes peuvent conforter un camp ou l'autre et renforcer les extrémismes. En revanche leur impact sur les électeurs indécis n'a jamais été mesuré clairement.

04. La désinformation

Dans leur lettre ouverte, ces experts déclarent à raison que « *Pour qu'une société moderne fonctionne, les gens doivent avoir accès à des informations crédibles et authentiques. Induire le public en erreur en utilisant l'IA devrait être réglementé et appliqué par des lois spécifiques et formalisées. Il devient de plus en plus difficile de savoir ce qui est réel sur Internet, et des lignes doivent être tracées pour protéger notre capacité à reconnaître de vrais êtres humains* »[141]. Mais les chercheurs Simon, Altay et Mercier, relativisent en soulignant que les sources d'information traditionnelles continuent d'occuper le haut du pavé et que les médias traditionnels restent la référence pour s'informer. Selon eux, le « *public qui s'informe à partir de médias alternatifs et qui "consomme" des fausses informations est déjà abreuvé de telles sources et ne recherche pas tant une information précise que des informations qui confirment leurs idées, fondées sur une méfiance généralisée vis-à-vis des politiques et des médias* »[142]. Il est vrai que quand Trump dit, en plein débat télévisé, contre Kamala Harris, que les immigrés envahissent nos villes, encouragés par les Démocrates qui les font venir pour les faire voter pour eux, ajoutant qu'ils mangent nos chiens et nos chats domestiques, il cherche essentiellement à conforter les complotistes et les anti-système.

Une photo truquée d'un meeting imaginaire de Kamala Harris, partagé par Donald Trump sur le réseau X.

Mais, au vu de l'augmentation exponentielle des deepfakes et de leur facilité de manipulation, on peut imaginer une explosion d'hypertrucages plus crédibles avec, par exemple, trois quarts de vrai et un quart de petits mensonges. Les fakes news les plus efficaces ont souvent utilisé une part de vrai. Dans ce cas, le mélange des genres risque de créer de la confusion malgré tout. En effet, en scrollant sur son réseau social, une personne peut voir défiler du vrai ou du faux ou les deux mélangés, sans prendre le temps de faire la part des choses. Démultiplier et décliner à l'infini le fake, à notre sens, c'est donner plus d'armes à la perte de repères informatifs.

En revanche, ce qui semble faire consensus, c'est la multiplication de deep propagande depuis l'étranger pour créer la confusion et entretenir la méfiance des citoyens d'un pays envers leurs pouvoirs politiques, juridiques ou médiatiques. Chine, Iran et Russie sont particulièrement actifs dans ce domaine. Sans parler des Évangélistes américains (91 millions de pratiquants aux USA[143]), grands défenseurs du créationnisme, d'un Donald Trump messianique, voire de l'Armageddon, que plusieurs millions[144] d'entre eux voient comme le lieu du combat final entre le Bien et le Mal à la fin du monde, lors du retour sur terre de Jésus-Christ en Israël.

05.Un flou artistique

« *En tant que membres du public, nous nous réjouissons des exploits de vrais artistes dans la danse, le cinéma, la magie, la musique, les sports et le théâtre. Si le divertissement diffusé devient saturé de deepfakes, le lien entre le public et les artistes s'érodera, et les deepfakes remplaceront injustement les artistes dont les œuvres ont été utilisées, à l'origine, pour "entraîner" l'IA* »[145]. Le risque est pris très au sérieux par les industries du disque et de la vidéo, qui vont certainement mettre des moyens importants pour défendre leurs droits d'auteurs sur des voix et des styles musicaux.

Et que vont devenir les musiciens quand il suffit de demander à l'IA de créer un morceau ou d'accompagner un air. Suffisamment alimenté en prompts, l'IA pourrait largement les remplacer, sans pour autant se substituer à la créativité ressentie d'un artiste. Aux États-Unis déjà, on tente de légiférer comme avec le No Fakes Act, visant à créer une loi fédérale pour protéger les acteurs, les musiciens et les autres artistes contre des répliques numériques non autorisées de leur visage ou de leur voix. « *Le projet de loi prévoit une exception pour l'utilisation de copies numériques à des fins de parodie, de satire et de critique. Il exclut également les activités commerciales telles que les publicités, pour autant qu'il s'agisse d'informations, d'un documentaire ou d'une parodie* »[146].

Autre grand problème, le dévoiement pornographique des images de célébrités qui peut être un frein à l'exposition publique des artistes. Nous l'avons vu, la Corée du Sud est au cœur du phénomène. En 2024, « *d'importants labels de K-pop, JYP Entertainment et ADOR, qui gèrent notamment les groupes Twice et NewsJeans, ont annoncé vouloir lancer des actions en justice pour protéger leurs artistes. Mais peu d'affaires aboutissent : entre 2021 et juillet 2024, 793 délits liés aux "deepfakes" ont été signalés, mais seulement seize personnes ont été arrêtées et poursuivies, selon les données de la police* »[147]. Et nous ne parlons ici que de la Corée du Sud.

À l'heure actuelle, il est en effet, difficile d'imaginer des poursuites efficaces contre ce genre de crimes, puisque réalisables depuis l'étranger, sans avoir besoin d'énormes moyens matériels et juridiques. On ne peut imaginer que la censure des grandes plateformes pour freiner leur succès, mais il se trouvera toujours un site pour les accueillir.

06.Pistes de solutions

La piste la plus répandue est celle d'un marquage numérique, une sorte de tatouage des images, indiquant qu'elles ont été fabriquées par une IA[148]. Selon la lettre, « *il est possible pour les caméras de générer des sceaux numériques infalsifiables sur des photographies et des vidéos non modifiées du monde réel, en utilisant des techniques de signature cryptographique similaires aux certificats de sites web et aux identifiants de connexion. S'ils étaient utilisés à grande échelle, ces sceaux permettraient à quiconque d'utiliser des applications d'authentification open source pour vérifier l'authenticité d'une photo ou d'une vidéo correctement signée. Les fabricants d'appareils, les développeurs de logiciels et les sociétés de médias devraient collaborer et populariser ces méthodes d'authentification du contenu ou d'autres méthodes similaires* ». Ajoutant « *les lois actuelles ne ciblent et ne limitent pas de manière adéquate la production et la diffusion de deepfakes, et même les exigences imposées*

aux créateurs - qui sont souvent mineurs - sont inefficaces. L'ensemble de la chaîne d'approvisionnement des "deepfakes" devrait être tenu pour responsable, comme c'est le cas pour les logiciels malveillants et la pédopornographie »[149]. Cela dit, le marquage numérique des deepfakes est une solution proposée par les géants du secteur mais il se trouvera toujours un site, quelque part dans le monde, pour contourner ces lois. Dans l'état actuel des choses, la Russie pourrait par exemple offrir un tel service aux utilisateurs européens ou américains pour chercher à y envenimer un peu plus les polarisations politiques et/ou idéologiques. C'est pourtant la seule piste réellement développée par les élites actuellement.

6. Comment encadrer le phénomène deepfake ?

01. Côté américain

De manière générale, les grandes plateformes semblent accepter les limites à la liberté d'expression en ce qui concerne les deepfakes images, particulièrement dans les domaines politiques et pornographiques.

- *« OpenAI, la société à l'origine de l'outil de génération d'images DALL-E, a déjà supprimé le contenu explicite de ses données et filtre les demandes de création d'images de célébrités et d'hommes politiques.*
- *Un autre modèle d'IA populaire, Midjourney, bloque certains mots-clés et encourage les utilisateurs à signaler les images problématiques aux modérateurs.*
- *TikTok a également imposé que les contenus manipulés soient étiquetés comme faux ou altérés, et a interdit les "deepfakes" de personnalités privées et de jeunes.*
- *Twitch a averti que la promotion, la création ou le partage intentionnels de "deepfakes" pornographiques entraîneraient un bannissement immédiat.*
- *Parallèlement, Meta, OnlyFans et Pornhub ont tous commencé à participer à un nouvel outil "Take It Down" permettant aux adolescents de signaler des images et des vidéos explicites d'eux-mêmes sur l'internet*[150]*. Cependant, les visages de vedettes transposées sur des films pornos sont encore légion sur un site comme Pornhub.*
- *Google a ajusté ses algorithmes pour minimiser l'affichage de contenus explicites et fallacieux parmi les résultats de recherches, en particulier lorsqu'une recherche mentionne des noms spécifiques associés à des deepfakes. La plateforme a aussi simplifié le processus de suppression de contenus, particulièrement pour les victimes de deepfakes, pour qui un filtrage sera mis en place afin de réduire l'exposition de la victime.*
- *Sensity dispose de son propre outil d'analyse des pixels et de la structure du fichier pour détecter s'il a été modifié.*
- *Intel a lancé un détecteur de deepfake en temps réel en 2022 qui inspecte la façon dont la lumière interagit avec les vaisseaux sanguins du visage.*
- *Les plates-formes Meta's étiquetteront bientôt le contenu généré par l'IA pour leurs utilisateurs »*[151].

Côté politique aussi les choses avancent. Le Sénat américain a, par exemple, adopté à l›unanimité un projet de loi fin juillet 2024, le Disrupt Explicit Forged Images and Non-Consensual Edit Act (DEFIANCE) Act, qui permet aux victimes de deepfakes sexuellement explicites de poursuivre au civil ceux qui ont produit ou traité l'image dans l'intention de la distribuer. La Californie, le Texas, le Wisconsin, l'État de Washington, le Minnesota ou encore le Michigan ont adopté une législation conçue pour lutter contre l'IA lors des élections. Les deep porns font également l'objet de lois et de poursuites judiciaires. Le président Joe Biden, lui-même a publié un ordre exécutif, en octobre 2023, chargeant le Département du Commerce de créer des conseils sur le contenu de l'IA « watermarking »[152] pour indiquer clairement que certaines vidéos deepfake n'ont pas été créées par des humains.

Le 16 février 2024, une vingtaine de grandes entreprises du numérique, parmi lesquelles Google, Meta, OpenAI, Microsoft, Amazon, X, IBM, TikTok, Adobe, Snap, ou encore Stability AI, ont signé un accord permettant « *d'aider à empêcher les contenus trompeurs générés par IA d'interférer dans les élections prévues cette année (2024, ndlr) dans le monde* »[153], dans le cadre du forum sur la sécurité de Munich. Elles s'engagent à développer des outils communs, notamment via des sortes de « tatouage numérique », lisibles par les machines. Un travail déjà en cours, avec, notamment, le standard C2PA[154] [155], pour Coalition for Content Provenance and Authenticity. Mais les termes du contrat manquent de clarté, notamment sur les réponses à apporter et sur le contexte du deepfake qui peut avoir des vertus éducatives, satiriques, politiques, artistiques ou autres. Les entreprises de la Tech ont également insisté sur le fait que cette lutte ne relevait pas de leur seule responsabilité : « *Nous nous engageons à faire notre part en tant qu'entreprises technologiques, tout en affirmant que l'usage trompeur de l'IA ne représente pas seulement un défi technique, mais un problème politique, social et éthique, et nous espérons que d'autres s'engageront également à agir dans le reste de la société* »[156].

02. La Chine, un parti, un récit

Avec le succès de l'application d'échange de visage Zao[157], devenue numéro un sur la liste des applications de divertissement gratuites dans l'App Store d'Apple dans les deux jours suivant ses débuts[158], le gouvernement chinois a décidé de prendre des dis-

positions radicales pour éviter toute dérive. Depuis janvier 2020 il est obligatoire de préciser qu'une vidéo a été créée grâce à l'intelligence artificielle et qu'elle rapporte de fausses informations, pour qu'elle soit publiée de manière légale. Si ces mentions n'apparaissent pas, le créateur de la deepfake sera considéré comme un criminel aux yeux des autorités chinoises et donc traité comme tel.

En Chine, on ne badine pas avec la « fausse propagande », ou du moins avec les informations non officielles, ni même avec la satire politique.

03. L'Europe crée des garde-fous

L'Union européenne a, de son côté, déjà voté son AI Act, début 2024, qui devrait entrer en vigueur en 2025. Le texte impose, entre autres, l'étiquetage des deepfakes (watermarking). Il y a également le code de bonnes pratiques 2022, élaboré par « *les principales plateformes en ligne, les plateformes émergentes et spécialisées, les acteurs du secteur de la publicité, les vérificateurs de faits, les organismes de recherche et les organisations de la société civile … contre la désinformation, conformément aux orientations de la Commission de mai 2021… Les signataires se sont engagés à prendre des mesures dans plusieurs domaines, tels que: démonétiser la diffusion de la désinformation; garantir la transparence de la publicité à caractère politique; donner aux utilisateurs les moyens d'agir; renforcer la coopération avec les vérificateurs de faits; et offrir aux chercheurs un meilleur accès aux données* »[159].

04. Côté belge

Dans le cas de deepfakes politiques, selon Sandrine Carneroli, avocate spécialiste en droit des médias à Bruxelles, « *si l'intention de son auteur est "de manipuler et de travestir la vérité politique, économique, sociale", ce dernier risque des sanctions. On peut faire valoir l'atteinte à la vie privée de la personne qui est présentée en disant des choses qui ne correspondent pas à ce qu'elle dirait en temps normal. On arrive dans ce qu'on appelle le délit de presse. On n'est plus sur la voie pénale parce qu'on va devoir analyser les propos* »[160]. Le contexte d'un deepfake reste donc au cœur de tout débat.

Dans le cas de deep porn, elle ajoute qu' « *On peut demander que le tribunal donne une injonction à la plateforme pour identifier l'auteur du contenu préjudiciable. Puisque la plateforme connaît les identifiants, a accès à un compte bancaire, etc. La loi permet également de faire une action en urgence, un référé, pour faire supprimer le contenu dans un délai de 6 heures, non seulement à l'auteur, s'il est connu, mais également au diffuseur, qui s'expose à une amende. Autre point intéressant souligné par l'avocate, le RGPD et "la loi belge d'application protègent les données nominatives, et l'image d'une personne est une donnée nominative" Une plainte pourrait ainsi être déposée auprès de l'Autorité de protection des données* ».

Depuis 2020, la loi sur le *revenge porn*, punit également la « diffusion non consensuelle d'images à caractère sexuel ».

05. Attention, tous les fakes ne sont pas égaux

Les deepfakes audio ont cet « avantage » sur les images, qu'ils sont plus difficiles à détecter, meilleurs marchés et plus facile à réaliser. On peut ainsi faire dire un mensonge à un présentateur de journal parlé ou à une personnalité politique en pleine campagne électorale.

Une vraie gageure pour les plateformes qui vont devoir les repérer pour se conformer, par exemple, au Code de pratique de l'UE en matière de désinformation. Renforcé en juin 2022, il interdit les Deepfakes et enjoint les plates-formes à utiliser leurs outils (modération, déplateformisation[161]…) pour s'en assurer.

Ces faux sonores, générées par l'IA, pourraient-ils être carrément mentionnés par une autre IA en réponse à une recherche de citoyen ? Pour l'éviter, il faudrait un marquage numérique à la production des faux sonores également et là-dessus, il n'y a pas encore d'information.

Ces contrôles pourraient être faits, dans une certaine mesure, par des journalistes spécialisés dans le *factchecking*. Mais les journalistes eux-mêmes sont inquiets des évolutions fulgurantes des deepfakes et font notamment appel, via Reporters sans Frontières, au corps juridique, pour la protection des journalistes, afin qu'ils créent un « délit de deepfake » capable de dissuader les manipulateurs[162]. De plus, les journalistes ne pourront vérifier que des infos d'actualités utiles mais il ne sera pas de leur ressort de vérifier les arnaques, utilisant une fausse voix, qui pullulent sur les réseaux. Les plateformes relayant ces faux ont, ici encore, clairement une responsabilité et un rôle à jouer dans leur filtrage.

06. Des outils d'aide se mettent en place

Par ailleurs, des outils en ligne comme Deepware Scanner, GPTZero, SynthID ou Copyleaks AI Détecteur de contenu, peuvent vous aider à repérer le contenu généré par l'IA – qu'il s'agisse de texte, d'images ou de vidéos[163].

Il est certain que d'autres outils de ce type vont se développer. L'un ou l'autre pourrait même supplanter les autres par son uni-

versalité et son efficacité à repérer les deepfakes. Mais il y a fort à parier que celui-ci devienne payant et n'aide que les plus nantis. Il devrait pourtant être un outil de service public.

Conclusion

Les deepfakes peuvent donc théoriquement avoir des conséquences diverses et entraîner diffamation, violation de propriété intellectuelle, violation de la vie privée et de la protection des données, harcèlement, fraude, chantage, violation de droits de publicitaires, interférence électorale ou encore incitation à la violence et aux troubles sociaux et civils.

Et, contrairement à la prise en main d'un outil comme Photoshop, plutôt complexe, les outils d'IA comme DALL-E et Midjourney, pour fabriquer une image, ou Sora, pour la vidéo, permettent de générer des contenus réalistes à partir de quelques mots clés. Il est donc urgent de porter à la connaissance du plus grand nombre, non seulement leur existence, mais aussi et surtout de leurs possibles et néfastes applications.

L'une des plus choquante est la réalisation de deep nudes, voire de deep porns, au sein d'écoles pour humilier et/ou racketter une fille, et plus rarement un garçon, de son entourage. Selon une enquête réalisée par l'Université d'Anvers, 7% des Belges entre quinze et vingt-cinq ans ont déjà tenté d'en réaliser un. Si on rapporte ce chiffre à la pyramide des âges de Statbel[164], cela représente près de cent mille jeunes qui ont créé un deep sexuel. Alors que beaucoup de parents et de professeurs n'ont pas encore vraiment entendu parler du phénomène qui explose, et pas seulement dans les écoles. Peu sont à l'abri car tant qu'une photo de quelqu'un est en ligne, sur un réseau social par exemple, il peut faire l'objet d'un deepfake. Et les gens en mettent par dizaines en ligne. Il est particulièrement urgent de porter ces perfectionnements abjects du harcèlement à la connaissance de tous et de sévir rapidement pour éviter une prolifération accompagnée d'un sentiment d'impunité, particulièrement chez les mineurs. Car aujourd'hui les poursuites restent rares. Le plus souvent, les victimes ne sont pas au courant de l'infraction, ou elles n'ont pas le courage ou les moyens de se confronter aux créateurs de ces vidéos. Certains mineurs ne distinguent même pas spécialement la différence entre ajouter des oreilles de lapin à la photo d'une fille de leur école et utiliser son visage pour en faire un deep nude. Pour eux, c'est juste marrant. Beaucoup d'hommes voient même les deep nudes comme une forme de satire. Il y a donc, en parallèle, un gros travail de conscientisation qui doit être fait pour que ces personnes prennent la mesure de la portée de leurs actes.

L'autre grand danger est clairement le perfectionnement des arnaques en ligne. Pourra-t-on encore croire ce qu'on voit et entend sur le net, sachant qu'un deepfake est toujours possible ? Comment sera-t-il possible de communiquer en toute confiance désormais avec son patron ou sa famille ? Via des VPN[165] ? Oui mais les meilleurs sont payants et les personnes ayant le moins de moyens risquent d'être plus exposés que les autres, alors qu'elles sont déjà fragilisées numériquement. L'arrivée de l'IA risque de complexifier encore plus les choses. Quelle que soit la réponse, l'État a le devoir de protéger ses citoyens mais il ne s'en donne pas assez les moyens. Rien qu'en ce qui concerne les cyber-attaques, « *plus de 60 % des professionnels européens de la cybersécurité déclarent que l'équipe de cybersécurité de leur organisation manque de personnel, et plus de la moitié (52 %) pensent que le budget de cybersécurité de leur organisation est insuffisant* ». L'arrivée de l'IA a clairement boosté ces chiffres et le nombre d'appareils connectés se multiplient pour donner toujours plus de données, exploitables par des escrocs du monde entier. Et désormais les deepfakes facilitent les vols d'identité.

Éviter une prolifération accompagnée d'un sentiment d'impunité

Il est certain qu'une concertation internationale devient essentielle pour partager les meilleures pratiques, légiférer et condamner dans le plus de pays possible. Mais il est difficile de croire que tous y participeront. D'ailleurs, si l'influence des deepfakes dans un processus électoral est encore rare et est rapidement dénoncée côté occidental, des pays moins démocratiques comme l'Inde, la Turquie ou le Vénézuela ont montré que l'outil permettait aux pouvoirs en place d'asseoir leur propagande et toucher les citoyens presque directement. C'est un énième outil de propagande, mais il peut être particulièrement efficace sur les populations non averties, en l'absence d'une presse indépendante notamment. Et l'IA ne fera que le perfectionner encore et encore. C'est là l'un des points d'attention pour les deepfakes politiques, punir les producteurs et responsabiliser les diffuseurs et les consommateurs. La justice aura également son rôle à jouer. En Europe, elle bénéficie de lois pour défendre les citoyens face à la désinformation, aux dérives de l'IA ou encore au vol de données. Et ce sera à la justice de déterminer la pertinence ou non d'une satire, du moins si on lui en donne les moyens.

Mais les pouvoirs publics ne doivent pas oublier qu'une des bases du problème est que la consommation de fausses informations est souvent motivée par des sentiments d'opposition envers les institutions et les corps sociaux établis, perçus comme ayant failli dans leur mission. La crise du Covid-19 en a fourni une illustration récente, avec l'émergence rapide de figures très médiatisées, en opposition frontale et systématique avec les mesures proposées,

et très soutenues par leurs supporters sur les médias sociaux. En 2023, la campagne présidentielle argentine a été « pimentée » par quelques deepfakes, comme celui de l'ex-président Massa en train de sniffer de la cocaïne. À la suite de quoi Natalia Zuazo, spécialiste argentine de la politique et des technologies, disait en interview : « *Ces contenus sont bon marché à produire et apportent de l'originalité à la campagne électorale, qui, d'ordinaire, en manque … La fake news n'a pas forcément besoin d'être convaincante pour qu'on la croit. Elle doit juste valider une croyance préexistante chez ce public qui brûle de voir quelque chose d'horrible chez le candidat qu'il rejette* »[166]. La diffusion de fausses informations créée ainsi un sentiment d'appartenance et de solidarité au sein de groupes qui s'opposent au pouvoir en place. Mais ces petits jeux peuvent aller loin. Verra-t-on un jour une campagne fondée sur des batailles de deepfakes en lieu et place d'arguments politiques ? Les deepfakes sont un élément de show supplémentaire aux élections polarisées auxquelles nous assistons de plus en plus de par le monde, quitte à flirter avec la calomnie et la diffamation.

Reste que le public devra être mis au courant des nouvelles technologies et de leurs opportunités d'utilisation trompeuse. Mais à l'heure actuelle, cela demande quasi une démarche proactive de la part des citoyens. Ils doivent trouver une formation ou un EPN, dont beaucoup ne connaissent même pas encore l'existence, monter dans le TGV du numérique et se protéger contre des escroqueries boostées à l'IA et pensées par des professionnels. C'est absurde, sachant qu'il y a déjà un gros travail pour réduire la fracture numérique et susciter l'intérêt pour la chose numérique, à l'heure où nombre de gens, toute classe sociale confondue, ne savent pas ce qu'est un cookie et s'en contrefichent.

> *Il faut toujours connaître les limites du possible. Pas pour s'arrêter, mais pour entreprendre l'impossible dans les meilleures conditions.*
>
> Romain Gary, *Charge d'âme*, 1977

[1] Courteille P., « Fakeland, un nouvel et obscur continent », Citoyenneté & Participation, Étude n°31, Avril 2020, [en ligne :] http://www.cpcp.be/publications/fakeland.

[2] Selon une étude de la revue Science parue en 2018. Démontrant que ces chiffres sont davantage dus aux humains qu'aux bots, ces logiciels réalisant seuls des opérations sur internet. Temming M., « On Twitter, the lure of fake news is stronger than the truth », Science News, 8 mars 2018, [en ligne :] (https://www.sciencenews.org/article/twitter-fake news-truth, consulté le 6 mars 2020.

[3] Cellan-Jones R., « Rory Cellan-Jones », BBC News Technology, 12 août 2016, [en ligne :] https://www.bbc.com/news/technology-37046477, consulté le 2 avril 2020.

[4] Vérification des faits, le plus souvent faite par des professionnels de l'info, comme des journalistes.

[5] Kessler G., « introducing fact checkers guide manipulated video », Washington Post, le 25 juin 2019, [en ligne :] https://www.washingtonpost.com/politics/2019/06/25/introducing-fact-checkers-guide-manipulated-video/, consulté le 2 avril 2020.

[6] La rédaction de Sumsub, « Sumsub Research : Le nombre d'incidents liés au Deepfake a décuplé entre 2022 et 2023 », Sumsub, le 28 novembre 2023, [en ligne :] https://sumsub.com/newsroom/sumsub-launches-advanced-deepfakes-detector, consulté le 2 avril 2024.

[7] Gaudiaut T., « Intelligence artificielle : les deepfakes explosent », Statista, le 18 mars 2024, [en ligne :] https://fr.statista.com/infographie/31929/pays-ayant-connu-les-plus-fortes-hausses-de-cas-de-deepfakes, consulté le 23 juillet 2024.

[8] AFP, « Face au tweet de Trump, Hillary Clinton répond par une réplique culte du film "Lolita malgré moi" », Le Soir, 6 mars 2019, [en ligne :] https://www.lesoir.be/210738/article/2019-03-06/face-au-tweet-de-trump-hillary-clinton-repond-par-une-replique-culte-du-film, consulté le 2 avril 2020.

[9] Ovadya A., « Quoi de pire que de fausses nouvelles ? La distorsion de la réalité elle-même. », The Washington Post, 22 février 2018, [en ligne :] https://www.washingtonpost.com/news/theworldpost/wp/2018/02/22/digital-reality/?noredirect=on, consulté le 18 septembre 2020.

[10] Laugée F., « Deepfake », La revue européenne des médias et du numérique, automne 2019, [en ligne :] https://la-rem.eu/2019/11/deepfake, consulté le 23 avril 2020.

[11] Wintics, « quand la data science devient creative avec les gan », Wintics, juin 2020, [en ligne :] http://wintics.com/fr/quand-la-data-science-devient-creative-avec-les-gan, consulté le 17 juin 2020.

[12] *Ibid.*

[13] Cuvelliez C., Emission radio « Les deepfakes : 5 questions pour comprendre comment faire dire n'importe quoi à n'importe qui », La Première – Culture (RTBF), lundi 17 juin 2019, [en ligne :] https://www.rtbf.be/lapremiere/article/detail_les-deepfakes-5-questions-pour-comprendre-comment-faire-dire-n-importe-quoi-a-n-importe-qui?id=10248164, consulté le 10 avril 2020.

[14] Reddit est un site web communautaire américain d'actualités sociales fonctionnant via le partage de signets permettant aux utilisateurs de soumettre leurs liens et de voter pour les liens proposés par les autres utilisateurs. Ainsi, les liens les plus appréciés du moment se trouvent affichés en page d'accueil. Fondé en 2005, Reddit contenait alors surtout du contenu sur la programmation et la science. Il ne cesse depuis de se diversifier et de s'ouvrir à du contenu plus grand public. Ayant connu une explosion de croissance en 2010, en 2020, il se place comme le vingtième site web le plus populaire au monde et le sixième aux États-Unis selon Alexa Internet.

[15] Ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine.

[16] Tual M., « Du porno aux fausses informations, l'intelligence artificielle manipule désormais la vidéo », Le Monde (Pixels), 04 février 2018, [en ligne :] https://www.lemonde.fr/pixels/article/2018/02/04/du-porno-aux-fausses-informations-l-intelligence-artificielle-manipule-desormais-la-video_5251535_4408996.html, consulté le 30 mars 2020.

[17] *Ibid.*

[18] Maillé P., « "Deepfake", quand le faux gagne la vidéo », Libération, 31 août 2018, [en ligne :] https://www.liberation.fr/futurs/2018/08/31/deepfake-quand-le-faux-gagne-la-video_1675699, consulté le 18 juillet 2019.

[19] Lemega C. et Ben Sassi P., « Deepfake, les visages du danger », M6 - Le Mag, 12h45, 12 mars 2019, [en ligne :] https://www.rtl.fr/actu/futur/video-les-deepfakes-ces-fake news-video-ultra-realistes-7797188493, consulté le 1 avril 2020.

[20] Buzzfeedvideo, « You Won't Believe What Obama Says In This Video! », YouTube, 17 avril 2018, https://www.YouTube.com/watch?v=cQ54GDm1eL0&feature=emb_logo, consulté le 20 mai 2020.

[21] Lesaffre C., « Attention, les « deepfake », des vidéos truquées, se multiplient sur le Net », Europe 1, 17 juin 2019, [en ligne :] https://www.europe1.fr/technologies/attention-les-deepfake-des-videos-truquees-se-multiplient-sur-le-net-3904942, consulté le 1 avril 2020.

[22] Desaunay D., « La menace du "deepfake" se précise », RFI, 14 juin 2019, [en ligne :] http://www.rfi.fr/fr/emission/20190615-menace-deepfake-precise, consulté le 31 mars 2020.

[23] Dont le professeur Michael Zollhöfer, professeur assistant invité à l'Université de Stanford, et ses collègues de l'Université technique de Munich, de l'Université de Bath, de Technicolor et d'autres institutions. Thies j., Zollhöfer M., Stamminger M., Theobalt C., Niebner M., « Face2face: Real-time Face Capture and reenactment of RGB Videos », YouTube, 2016, [en ligne :] https://www.YouTube.com/watch?v=ohmajJTcpNk, consulté le 9 avril 2020.

[24] Toussaint C. avec AFP, « Les vidéos "deepfakes" se perfectionnent et inquiètent les chercheurs », RTBF, 11 septembre 2019, [en ligne :] https://www.rtbf.be/info/societe/detail_les-videos-deepfakes-se-perfectionnent-et-inquietent-les-chercheurs?id=10312839, consulté le 9 avril 2020.

[25] Cole S., « Ce programme open-source vous permet de profiter des réunions Zoom, en temps réel », Vice, 16 avril 2020, [en ligne :] https://www.vice.com/en_us/article/g5xagy/this-open-source-program-deepfakes-you-during-zoom-meetings-in-real-time, consulté le 20 avril 2020.

[26] Grand H., « Après les fake news, la menace du "deep fake" prend de l'ampleur sur le web », Le Figaro Tech&Web, 2 janvier 2019, [en ligne :] https://www.lefigaro.fr/secteur/high-tech/2019/01/02/32001-20190102ARTFIG00162-apres-les-fake news-la-menace-du-deep-fake-prend-de-l-ampleur-sur-le-web.php, consulté 10 avril 2020.

[27] Laugée F., « Deepfake », La revue européenne des médias et du numérique, automne 2019, *op. cit.*

[28] The Dali Museum, « Behind the Scenes: Dalí Lives », YouTube, [en ligne :] https://www.YouTube.com/watch?v=BIDaxl4xqJ4&t=178s, consulté le 20 août 2024.

[29] Tondeur C., « Un Belge, derrière les deepfake de Tom Cruise », RTBF, le 8 mars 2021, [en ligne :] https://www.rtbf.be/article/un-belge-derriere-les-deepfake-de-tom-cruise-10714393, consulté le 20 août 2024.

[30] Dekock C., « Chris Umé, ce Belge qui a bluffé l'Amérique en faisant chanter un air d'opéra aux jurés d'America's got Talent », RTBF, le 2 septembre 2022, [en ligne :] https://www.rtbf.be/article/chris-ume-ce-belge-qui-a-bluffe-l-amerique-en-faisant-chanter-un-air-d-opera-aux-jures-d-america-s-got-talent-11058573, consulté le 20 août 2024.

[31] Voir extrait sur YouTube, [en ligne :] https://www.YouTube.com/watch?v=rJfwx8iZel0, consulté le 20 août 2024.

[32] Reynaud F. et Croquet P., « TikTok et le business des récits de faits divers dopés au deepfake », Le Monde, le 27 février 2024, [en ligne :] https://www.lemonde.fr/pixels/article/2024/02/27/tiktok-et-le-business-des-recits-de-faits-divers-dopes-au-deepfake_6218894_4408996.html, consulté le 20 aout 2024.

[33] Rochefort M., « Des influenceurs générés par l'IA pourraient bientôt envahir TikTok », Siècle Digital, le 12 avril 2024, [en ligne :] https://siecledigital.fr/2024/04/12/des-influenceurs-generes-par-lia-pourraient-bientot-envahir-tiktok, consulté le 21 août 2024.

[34] IA School, « Quels sont les dangers du phénomène deepfake ? », IA School, [en ligne :] https://www.intelligence-artificielle-school.com/ecole/technologies/quels-sont-les-dangers-deepfake, consulté le 17 août 2024.

[35] Comme nous le soulignions dans notre précédente étude de Philippe Courteille, « Fakeland, un nouvel et obscur continent », Citoyenneté & participation, Étude n°31, Avril 2020, [en ligne :] http://www.cpcp.be/publications/fakeland.

[36] De Buissiere Z., Thiebaut S. et Collot G., « Fake news : fausses infos et vrais bénéfices », France 2 - Complément d'enquête, le 23 mars 2017, [en ligne :] https://www.francetvinfo.fr/monde/usa/video-fake news-fausses-infos-et-vrais-benefices_2107586.html?fbclid=IwAR3JEmkRmNeqH_oI8pxrzmxOj1KaYLmZAfc92y-NL7hl0kgbgpnn1qufUH4, consulté le 16 juillet 2019.

[37] À sa mort en 2017, beaucoup ont cru à un fake. Il serait mort dans son lit d'une overdose de médicament, de quoi alimenter encore une quelconque théorie du complot. Kulwin N., « Un cocktail de fentanyl a tué le faux journaliste qui prétendait faussement avoir élu Trump », Vice, le 6 déc.2017, [en ligne :] https://news.vice.com/en_ca/article/d3xx7v/a-fentanyl-cocktail-killed-fake news-writer-paul-horner, consulté le 16 juillet 2019.

[38] Saint-Léger A., « Elon Musk drogué ? Un deepfake donne de la voix sur les réseaux sociaux », France 24, le 12 janvier 2024, [en ligne :] https://www.france24.com/fr/%C3%A9missions/info-ou-intox/20230112-un-deepfake-d-elon-musk-drogu%C3%A9-devient-viral, consulté le 17 août 2024.

[39] Ferraris S., « Sur Instagram, des influenceurs IA utilisent des deepfakes pour gagner des abonnés », BFM Tech&Co, le 10 avril 2024, [en ligne :] https://www.bfmtv.com/tech/instagram/sur-instagram-des-influenceurs-ia-utilisent-des-deepfakes-pour-gagner-des-abonnes_AV-202404100592.html, consulté le 12 juillet 2024.

[40] Stupp C., « Des fraudeurs ont utilisé l'IA pour imiter la voix du PDG dans une affaire de cybercriminalité inhabituelle », The Wall Street Journal, 30 août 2019, [en ligne :] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, consulté le 14 mai 2020.

[41] Brasseur T., « Des fraudeurs ont cloné la voix du directeur d'entreprise dans un braquage de banque de 35 millions de dollars, selon la police », Foirbes, 14 octobre 2021, [en ligne :] https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=4b47e9097559, consulté le 26 juillet 2022.

[42] Un brouteur est un escroc opérant sur Internet, notamment sur les réseaux sociaux. L'idée du « broutage », consiste à se faire envoyer de l'argent en faisant croire à une relation amoureuse ou amicale, totalement feinte en réalité.

[43] La redaction de LLB, « Des faux Brad Pitt extorquent près de 325 000 euros à des femmes en situation de vulnérabilité », La Libre Belgique, le 25 septembre 2024, [en ligne :] https://www.lalibre.be/international/europe/2024/09/25/des-faux-brad-pitt-extorquent-pres-de-325-000-euros-a-des-femmes-en-situation-de-vulnerabilite-MWX7HL-ZPWVFG7B64RBQ6IFSG4M, consulté le 24 juillet 2024.

[44] Davet S., « Quand l'intelligence artificielle crée des "deepfakes" musicaux », Le Monde, le 11 octobre 2023, [en ligne :] https://www.lemonde.fr/culture/article/2023/10/11/quand-l-intelligence-artificielle-cree-des-deepfakes-musicaux_6193851_3246.html, consulté le 2 août 2024.

[45] Robertson D., « It's the screams of the damned!' The eerie AI world of deepfake music », The Guardian, le 9 novembre 2020, [en ligne :] https://www.theguardian.com/music/2020/nov/09/deepfake-pop-music-artificial-intelligence-ai-frank-sinatra, consulté le 2 août 2024.

[46] La rédaction du Figaro, « Des fans créent un album d'Oasis grâce à l'intelligence artificielle », Le Figaro, avril 2023, [en ligne :] https://www.lefigaro.fr/musique/des-fans-creent-un-album-d-oasis-grace-a-l-intelligence-artificielle-20230420, consulté le 2 août 2024.

[47] Basdevant A., Camille François C., Ronfard R., « Mission exploratoire sur les métavers », Mission exploratoire pour le Gouvernement Français, octobre 2022, [en ligne :] https://www.economie.gouv.fr/files/files/2022/Rapport-interministeriel-metavers.pdf, consulté le 2 août 2024.

[48] Perez C. et Derhy A., « Métavers : l'heure du premier bilan », The Conversation, janvier 2023, [en ligne :] https://theconversation.com/metavers-lheure-du-premier-bilan-197149, consulté le 3 août 2024.

[49] Garnier A., « L'avenir du télétravail est dans le métavers », Le Point, le 30 septembre 2024, [en ligne :] https://www.lepoint.fr/debats/l-avenir-du-teletravail-est-dans-le-metavers-30-09-2022-2491914_2.php, consulté le 4 août, 2024.

[50] Blackburn M.R. et Hogg R.C., « Pour vous, l'impact du contenu pro-ana TikTok sur l'insatisfaction de l'image corporelle et l'internalisation des normes de beauté sociétales », Plos One, le 7 août 2024, [en ligne :] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0307597, consulté le 12 août 2024.

[51] Wiart L., « L'hyperconnexion au détriment de la conversation », La revue des médias, le 4 mars 2019, [en ligne :] https://larevuedesmedias.ina.fr/lhyperconnexion-au-detriment-de-la-conversation, consulté le 13 août 2024.

[52] Lamort E., « “Parler” à un proche disparu, cette nouvelle illusion inquiétante de l’intelligence artificielle », Ouest France, le 2 mai 2023, [en ligne :] https://www.ouest-france.fr/leditiondusoir/2023-05-02/parler-a-un-proche-disparu-cette-nouvelle-illusion-inquietante-de-l-intelligence-artificielle-6abba44f-1fdb-4a22-a605-df54a9a712f5, consulté le 12 août 2024.

[53] *Ibid.*

[54] *Ibid.*

[55] Bryce A.L., « Communiquer avec les morts grâce à l’Intelligence artificielle », EuroNews, 16 mars 2023, [en ligne :] https://fr.euronews.com/next/2023/03/16/communiquer-avec-les-morts-grace-a-lintelligence-artificielle, consulté le 12 août 2024.

[56] Kahn S., « “Le sida, c’est fini”: Solidarité Sida créé un deepfake de Donald Trump pour une campagne », Le Figaro Tech&Web, le 7 octobre 2019, [en ligne :] https://www.lefigaro.fr/secteur/high-tech/le-sida-c-est-fini-solidarite-sida-cree-un-deepfake-de-donald-trump-pour-une-campagne-20191007, consulté le 26 juillet 2024.

[57] Tual M., « Fausse vidéo de Trump : pourquoi Solidarité sida a sorti un “deepfake” pour sa campagne », Le Monde, le 9 octobre 2019, https://www.lemonde.fr/pixels/article/2019/10/09/fausse-video-de-trump-pourquoi-solidarite-sida-a-sorti-un-deepfake-pour-sa-campagne_6014864_4408996.html, consulté le 26 juillet 2024.

[58] Farcis S., « Les Indiens, terrorisés par les enlèvements d’enfants, alimentent les rumeurs », 16 juin 2018, [en ligne :] https://www.rfi.fr/fr/asie-pacifique/20180615-inde-reseaux-sociaux-rapt-enfants, consulté le 26 juillet 2024.

[59] Honnet T., « La danse d’(une fausse) Elizabeth II, ou la vidéo de lèse-majesté qui scandalise les Britanniques », Madame Figaro, décembre 2020, [en ligne :] https://madame.lefigaro.fr/celebrites/la-danse-tiktok-elizabeth-ii-qui-indigne-le-royaume-uni-video-deepfake-291220-194274, consulté le 27 juillet 2024.

[60] MIT Open Learning, « Tackling the misinformation epidemic with “In Event of Moon Disaster” », MIT News, juillet 2020, [en ligne :] https://news.mit.edu/2020/mit-tackles-misinformation-in-event-of-moon-disaster-0720 , consulté le 16 août 2024.

[61] MIT Open Learning, « In Event Of Moon Disaster Movie Trailer », YouTube, juillet 2020, [en ligne :] https://www.YouTube.com/watch?v=kc_ufCSQLwI&t=56s, consulté le 16 août 2024.

[62] Sondage IFOP, « Enquête sur le complotisme », IFOP, le 8 janvier 2018, [en ligne :] https://www.ifop.com/publication/enquete-sur-le-complotisme/, consulté le 12 août 2024.

[63] Biourge C., « L’intelligence artificielle : une menace de plus en plus importante pour l’information et un défi pour les journalistes », RTBF Info, le 3 mai 2023, [en ligne :] https://www.rtbf.be/article/l-intelligence-artificielle-une-menace-de-plus-en-plus-importante-pour-l-information-et-un-defi-pour-les-journalistes-11192380, consulté le 21 août 2024.

[64] Wagon L., « Une œuvre générée par IA lauréate d’un prix de photographie », Le Journal des Arts, le 20 avril 2023, [en ligne :] https://www.lejournaldesarts.fr/creation/une-oeuvre-generee-par-ia-laureate-dun-prix-de-photographie-166032, consulté le 21 août 2024.

[65] Une image deep porn de Taylor Swift a fait … 47 millions de vues. La chanteuse est connue pour ses positions anti Donald Trump et il y a fort à parier qu’il s’agit là d’une attaque des partisans de l’ancien président.

[66] Jacquet T., « Deepfakes pornographiques, politiques, économiques : quelles sont les sanctions prévues par le droit belge contre ces pratiques ? », RTBF, le 14 février 2023, [en ligne :] https://www.rtbf.be/article/deepfakes-pornographiques-politiques-economiques-quelles-sont-les-sanctions-prevues-par-le-droit-belge-contre-ces-pratiques-11151913, consulté le 19 juillet 2024.

[67] Hess A., « “La honte doit changer de camp” : une mannequin belge alerte sur les deepnudes », Euronews, 14 mars 2024, https://fr.euronews.com/next/2024/03/14/la-honte-doit-changer-de-camp-une-mannequin-belge-alerte-sur-les-deepnudes, consulté le 10 octobre 2024.

[68] Journal officiel de l’Union européenne, « DIRECTIVE (UE) 2024/1385 DU PARLEMENT EUROPÉEN ET DU CONSEIL, sur la lutte contre la violence à l’égard des femmes et la violence domestique », le Journal officiel de l’Union Européenne, le 14 mai 2024, [en ligne :] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401385, consulté le 20 juillet 2024.

[69] Hess A., *op. cit.*

[70] La rédaction de RTL Info, « Une ex-Miss Belgique victime de “deepnude” témoigne : “J’ai été profondément choquée” », RTL Info, le 6 octobre 2023, [en ligne :] https://www.rtl.be/people/news/une-ex-miss-belgique-victime-de-deepnude-temoigne-jai-ete-profondement-choquee/2023-10-06/article/595323, consulté le 13 août 2024.

[71] Blog Vidéo

[72] La rédaction de Midi Libre, « “C’est vraiment dégueulasse” : Léna Situations victime de deepfake porno, l’influenceuse témoigne de son écœurement », Midi Libre, le 11 août 2023, [en ligne :] https://www.midilibre.fr/2023/08/11/cest-vraiment-degueulasse-lena-situations-victime-de-deepfake-porno-linfluence-temoigne-de-son-ecoeurement-11391227.php, consulté le 20 juillet 2024.

[73] Bordecq C., « Victime de deepfake porno, la streameuse QTCinderella remet en lumière le phénomène des cyberviolences », RTBF, le 15 février 2023, [en ligne :] https://www.rtbf.be/article/victime-de-deepfake-porno-la-streameuse-qtcinderella-remet-en-lumiere-le-phenomene-des-cyberviolences-11153166, consulté le 20 juillet 2024.

[74] Hulstaert E., « Fake porno: comment les “deepnudes” détruisent la vie de Belges », Le Vif, le 13 août 2024, [en ligne :] https://www.levif.be/societe/fake-porno-comment-les-deepnudes-detruisent-la-vie-de-belges/, consulté le 16 août 2024.

[75] Bureau Web d’INDIA TODAY, « I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot », India Today, 21 novembre 2018, [en ligne :] https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21, consulté le 1 septembre 2020.

[76] Ayyub R., « J’ai été victime d’une vidéo porno truquée et d’un complot destiné à me faire taire », huffingtonpost, 2 décembre 2018, [en ligne :] https://www.huffingtonpost.fr/rana-ayyub/j-ai-ete-victime-d-une-video-porno-truquee-et-dun-complot-destine-a-me-faire-taire_a_23603520, consulté le 2 avril 2019.

[77] Bonte A., « “Deepfake” : Scarlett Johansson met en garde contre cet inquiétant phénomène », RTL France, 04 janvier 2019, [en ligne :] https://www.rtl.fr/girls/societe/deepfake-scarlett-johansson-met-en-garde-contre-cet-inquietant-phenomene-7796128802, consulté le 3 avril 2020.

[78] Hulstaert E., « Fake porno: comment les “deepnudes” détruisent la vie de Belges », *op. cit.*

[79] Huttin C., « Harcèlement scolaire : 280 écoles sont invitées à lutter contre ce “fléau” », Le Soir, le 10 février 2024, [en ligne :] https://www.lesoir.be/567489/article/2024-02-10/harcelement-scolaire-280-ecoles-sont-invitees-lutter-contre-ce-fleau, consulté le 28 août 2024.

[80] Hildesheim M., « Une dizaine de jeunes filles élèves du collège Saint-Remacle de Stavelot victimes de deepfakes », RTBF Info, le 21 juin 2024, [en ligne :] https://www.rtbf.be/article/une-dizaine-de-jeunes-filles-eleves-du-college-saint-remacle-de-stavelot-victimes-de-deepfakes-11392755, consulté le 3 septembre 2024.

[81] Llach L., « Des adolescents espagnols ont reçu des nus d’eux-mêmes générés par l’IA: s’agit-il d’un crime ? », Euronews, le 20 septembre 2023, [en ligne :] https://fr.euronews.com/next/2023/09/20/des-adolescents-espagnols-ont-recu-des-nus-deux-memes-generes-par-lia-sagit-il-dun-crime, consulté le 20 juillet 2024.

[82] *Ibid.*

[83] Llach L., *op. cit.*

[84] Hulstaert E., « Fake porno: comment les “deepnudes” détruisent la vie de Belges », *op. cit.*

[85] En fait avec la tête de Bruno Ganz jouant Adolf Hitler dans le film de 2004 « Downfall ».

[86] Mathiot C., Moullot P., Leboucq F., Pezet J., Andraca R., Coquaz V., « L’ivresse de la deepfake – Désintox », ARTE, Juin 2019, [en ligne :] https://www.YouTube.com/watch?v=nrNzG2yQqOA, consulté le 19 juillet 2019.

[87] La rédaction du Monde, « Deepfake de Joe Biden : l’identité du commanditaire dévoilée », Le Monde, le 26 février 2024, [en ligne :] https://www.lemonde.fr/pixels/article/2024/02/26/deepfake-de-joe-biden-l-identite-du-commanditaire-devoilee_6218633_4408996.html, consulté le 17 août 2024.

[88] Bensinger K., « Elon Musk Shares Manipulated Harris Video, in Seeming Violation of X’s Policies », The NYTimes, le 27 juillet 2024, [en ligne :] https://www.nytimes.com/2024/07/27/us/politics/elon-musk-kamala-harris-deepfake.html, consulté le 18 août 2024

[89] L’État profond (de l’anglais deep state) fait référence à l’idée qu’il existerait au sein d’un État une entité informelle détenant secrètement le pouvoir décisionnel sur la société.

[90] L’équipe de « C quoi l’info ? », « Amandine Le Pen, Lena Maréchal Le Pen… Mais qui sont ces fakes ? », YouTube, le 12 avril 2024, [en ligne :] https://www.YouTube.com/watch?v=nNyyPYYut1I&t=31s, consulté le 20 août 2024.

[91] La rédaction de France Info, « Amandine Le Pen, Lena Maréchal… Quels sont ces deepfakes qui poussent à voter pour l’extrême droite ? », France Info, le 12 avril 2024, [en ligne :] https://www.francetvinfo.fr/l-actu-pour-les-jeunes/marine-le-pen-marion-marechal-mais-qui-sont-ces-fakes-d-extreme-droite-regardez-le-nouveau-numero-de-c-quoi-l-info_6482963.html, consulté le 20 août 2024.

[92] Frau-Meigs D., « Deepfakes, vidéos truquées, n’en croyez ni vos yeux ni vos oreilles ! », The Concersation et RFI, le 10 juillet 2024, [en ligne :] https://www.rfi.fr/fr/connaissances/20240710-deepfakes-vid%C3%A9os-truqu%C3%A9es-n-en-croyez-ni-vos-yeux-ni-vos-oreilles, consulté le

[93] Herrera Y., « Venezuela : de faux JT présentés par des avatars prêchent la parole du gouvernement chaviste », Libération, le 21 février 2023, [en ligne :] https://www.liberation.fr/international/amerique/venezuela-de-faux-jt-presentes-par-des-avatars-prechent-la-propagande-de-nicolas-maduro-20230221_EEFBBHGKT5AC-TEBVKDOQAPRCZM/, consulté le 21 août 2024.

[94] Kansara R. et Krygier R., « Venezuela: ‚I’m paid to tweet state propaganda’ », BBC, le 26 mai 2023, [en ligne :] https://www.bbc.com/news/blogs-trending-65622685, consulté le 22 août 2024.

[95] La rédaction numérique de France Inter et AFP, « Présidentielle en Turquie : la campagne polluée par les “deepfakes”, les infox et les montages », France Inter, le 12 mai 2023, [en ligne :] https://www.radiofrance.fr/franceinter/presidentielle-en-turquie-la-campagne-polluee-par-les-deepfakes-les-infox-et-les-montages-5450979, consulté le 23 août 2024.

[96] D’après Reporter Sans Frontière, le pouvoir turc contrôlerait 90 % des médias nationaux.

[97] Jones D., « Deepfake videos used in local elections in Turkey as Erdogan battles for Istanbul », RFI, le 16 mars 2023, [en ligne :] https://www.rfi.fr/en/podcasts/international-report/20240316-deepfake-videos-used-in-local-elections-in-turkey-as-erdogan-battles-for-istanbul, consulté le 26 août 2024.

[98] *Ibid.*

[99] AFP, « Fake experts drive disinformation before Bangladesh polls », France 24, le 7 septembre 2023, [en ligne :] https://www.france24.com/en/live-news/20230907-fake-experts-drive-disinformation-before-bangladesh-polls, consulté le 27 août 2024.

[100] La redaction de l’Union Interpalementaire, « Dangers des “deepfakes” pour les parlementaires », UIP, le 21 février 2024, [en ligne :] https://www.ipu.org/fr/actualites/actualites-en-bref/2024-02/dangers-des-deepfakes-pour-les-parlementaires, consulté le 25 août 2024.

[101] Landrin S., « En Inde, des élections dopées aux deepfakes », Le Monde, le 20 mai 2024, [en ligne :] https://www.lemonde.fr/pixels/article/2024/05/20/en-inde-des-elections-dopees-aux-deepfakes_6234465_4408996.html, consulté le 25 août 2024.

[102] Raj S., « How A.I. Tools Could Change India’s Elections », New-York Times, le 18 avril 2024, [en ligne :] https://www.nytimes.com/2024/04/18/world/asia/india-election-ai.html, consulté le 26 août 2024.

[103] Entretien avec Obin N., « Deepfake : menace ou opportunité ? », Sorbonne Université, le 29 février 2024, [en ligne :] https://www.sorbonne-universite.fr/actualites/deepfake-menace-ou-opportunite, consulté le 26 août 2024.

[104] Le candidat Yoon de chair et d’os a enregistré plus de 3 000 phrases, soit vingt heures d’audio et de vidéo, pour fournir suffisamment de données à une entreprise sud-coréenne de technologie deepfake chargée de créer l’avatar.

[105] La rédaction d’Euronews avec AFP, « En Corée du Sud, un avatar “deepfake” pour booster la campagne d’un candidat », Euronews, le 14 février 2022, [en ligne :] https://fr.euronews.com/2022/02/14/en-coree-du-sud-un-avatar-deepfake-pour-booster-la-campagne-d-un-candidat, consulté le 3 août 2022.

[106] Rocca N., « Corée du Sud: Yoon Suk-yeol, prochain président, un K-Trump ? », RFI, 10 mars 2022, [en ligne :] https://www.rfi.fr/fr/asie-pacifique/20220310-cor%C3%A9e-du-sud-yoon-suk-yeol-prochain-pr%C3%A9sident-un-k-trump, consulté le 3 août 2022.

[107] Beurnez V., « Piratée, une chaîne d'information ukrainienne diffuse un "deepfake" de Volodymyr Zelensky », BFM Tech&Co, le 17 mars 2022, [en ligne :] https://www.bfmtv.com/tech/piratee-une-chaine-d-information-ukrainienne-diffuse-un-deepfake-de-volodymyr-zelensky_AN-202203170296.html, consulté le 17 septembre 2024.

[108] Biourge C., « L'intelligence artificielle : une menace de plus en plus importante pour l'information et un défi pour les journalistes », *op. cit.*

[109] d'Otreppe B., « Les risques des "fake news": "Même une information que l'on sait fausse nous influencera" », La Libre Belgique, 29 octobre 2018, [en ligne :] https://www.lalibre.be/belgique/2018/10/29/les-risques-des-fake news-meme-une-information-que-lon-sait-fausse-nous-influencera-H2M3NPDKENB4R-L5CEXSNYTGYZM, consulté le 31 mars 2020.

[110] Owono J., « Les "deepfakes", arme de désinformation massive », Jeune Afrique, 11 avril 2019, [en ligne :] https://www.jeuneafrique.com/mag/760688/societe/tribune-les-deepfakes-arme-de-desinformation-massive/, consulté le 31 mars 2020.

[111] À la veille des élections américaines de 2016, Donald Trump avait défrayé la chronique avec une vidéo de 2005 dans laquelle il tenait des propos obscènes. Juste avant une interview pour NBC, oubliant qu'il a un micro-cravate, il parle dans un bus de son rapport avec les femmes. Extraits : « "J'ai essayé de me la faire, elle était mariée", "Je suis automatiquement attiré par les belles, je les embrasse tout de suite" ... il explique notamment qu'être une star lui permet de faire "tout ce qu' [il] veut" avec les femmes, notamment les "attraper" par la "chatte" ». Cet enregistrement avait fait scandale. Aujourd'hui, les pro-Trump auraient désormais beau jeu de crier au deepfake pour discréditer l'info.

[112] AFP, « Autriche: démission de tous les ministres d'extrême droite », Le Soir, 20 mai 2019, [en ligne :] https://www.lesoir.be/225482/article/2019-05-20/autriche-demission-de-tous-les-ministres-dextreme-droite, consulté le 18 juillet 2020.

[113] Jeangène Vilmer J-B., Escorcia a., Guillaume M., Herrera J., « LES MANIPULATIONS DE L'INFORMATION - Un défi pour nos démocraties », France Diplomatie, 4 septembre 2018, [en ligne :] https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/manipulations-de-l-information/rapport-conjoint-caps-irsem-les-manipulations-de-l-information-un-defi-pour-nos, consulté le 12 mai 2020.

[114] Jeangène Vilmer J-B., Escorcia a., Guillaume M., Herrera J., *op. cit.*

[115] Saint-Léger A., « France 24 victime d'un "deepfake" : l'intox continue à circuler sur le web ! », France 24, le 16 février 2024, [en ligne :] https://www.france24.com/fr/%C3%A9missions/info-ou-intox/20240216-france-24-victime-d-un-deepfake-l-intox-continue-%C3%A0-circuler-sur-le-web, consulté le 24 juillet 2024.

[116] Nilesh C., « Nous venons de voir la première utilisation de Deepfakes dans une campagne électorale indienne », Vice Magazine, 18 février 2020, [en ligne :] https://www.vice.com/en_in/article/jgedjb/the-first-use-of-deepfakes-in-indian-election-by-bjp, consulté le 30 avril 2020.

[117] Arvind Kejriwal, qui a finalement remporté l'élection régionale de la capitale indienne.

[118] La rédaction du Courrier International, « États-Unis. L'IA utilisée pour créer de fausses images de Trump entouré de Noirs », Courrier International, le 11 mars 2024, [en ligne :] https://www.courrierinternational.com/article/etats-unis-de-fausses-images-de-trump-entoure-de-noirs-pour-seduire-cet-electorat, consulté le 19 juillet 2024.

[119] L'extrême-droite américaine.

[120] Mendoza N., « Italie : ces "fake news" qui parasitent la campagne des Européennes », France 24, le 22 mai 2019, [en ligne :] https://www.france24.com/fr/20190522-italie-europeennes-fake news-infox-ligue-salvini-migrants-facebook, consulté le 27 juillet 2024.

[121] Jeangène Vilmer J-B., Escorcia A., Guillaume M., Herrera J., « LES MANIPULATIONS DE L'INFORMATION - Un défi pour nos démocraties », *op. cit.*

[122] Goldenberg S., « Prenez une partie Kerry, une partie Fonda ... et essayez de susciter une polémique politique », The Guardian, 18 février 2004, [en ligne :] https://www.theguardian.com/media/2004/feb/18/newmedia.uselections2004, consulté le 20 mai 2020.

[123] AFP, « YouTube instaure des mesures pour mettre fin à la désinformation sur les avortements », Lapresse.ca, 21 juillet 2022, [en ligne :] https://www.lapresse.ca/affaires/techno/2022-07-21/YouTube-instaure-des-mesures-pour-mettre-fin-a-la-desinformation-sur-les-avortements.php, consulté le 8 août 2022.

[124] Leloup D., « Avortement illégal aux Etats-Unis : Facebook critiqué pour avoir fourni à la justice des messages privés », Le Monde, 11 août 2022, [en ligne :] https://www.lemonde.fr/pixels/article/2022/08/11/avortement-illegal-aux-etats-unis-facebook-critique-pour-avoir-fourni-a-la-justice-des-messages-prives_6137767_4408996.html, consulté le 22 août 2022.

[125] Signoret P., « Censure de "L'Origine du monde" : une faute de Facebook reconnue, mais pas sur le fond », Le Monde, le 15 mars 2018, [en ligne :] https://www.lemonde.fr/pixels/article/2018/03/15/censure-de-l-origine-du-monde-une-faute-de-facebook-reconnue-mais-pas-sur-le-fond_5271666_4408996.html, consulté le 8 août 2024.

[126] Cuny D. et O'neil C., « Les algorithmes peuvent creuser les inégalités et saper la démocratie », Nouvel Obs, 21 novembre 2016, [en ligne :] https://www.nouvelobs.com/rue89/rue89-le-grand-entretien/20160826.RUE3093/les-algorithmes-peuvent-creuser-les-inegalites-et-saper-la-democratie.html, consulté le 8 août 2022.

[127] Gillet E., « Numérisation du recrutement et de l'orientation. Promesses et conséquences des algorithmes », Citoyenneté & Participation, Analyse n°472, juin 2023, [en ligne :] https://www.cpcp.be/publications/numerisation-recrutement/, consulté le 10 juillet 2023.

[128] Entretien avec Obin N., « Deepfake : menace ou opportunité ? », *op. cit.*

[129] La redaction de l'Union Interpalementaire, « Dangers des "deepfakes" pour les parlementaires », *op. cit.*

[130] N'hésitez pas à essayer : [en ligne :] https://www.rtbf.be/article/ia-or-not-ia-arriverez-vous-a-reperer-les-images-generees-par-l-intelligence-artificielle-dans-ce-quiz-interactif-11227306.

[131] Sur le site internet de l'OTAN, on peut d'ailleurs lire : « Les cybermenaces et les cyberattaques deviennent de plus en plus fréquentes, sophistiquées et dommageables. L'Alliance est confrontée à un environnement de menaces complexes en pleine évolution. Lors de récents événements, des cyberattaques ont été utilisées dans le cadre d'actions de guerre hybride. L'OTAN et ses Alliés s'appuient sur des moyens de

cyberdéfense forts et résilients pour remplir les tâches fondamentales de l'Alliance que sont la défense collective, la gestion de crise et la sécurité coopérative. L'Alliance doit être préparée à défendre ses réseaux et opérations contre les cybermenaces et les cyberattaques toujours plus complexes auxquelles elle est confrontée. ». OTAN, « Cyberdéfense », OTAN, 31 May. 2018, [en ligne :] https://www.nato.int/cps/fr/natohq/topics_78170.htm, consulté le 16 septembre 2019, consulté le 21 avril 2020.

[132] Redaction De L'armee De Terre Française, « Entrez dans la nouvelle ère numérique de l'armée de Terre », Défense française, 2018, [en ligne :] https://www.defense.gouv.fr/web-documentaire/ere_numerique/index.html, consulté le 21 avril 2020.

[133] Jeangène Vilmer J-B., Escorcia A., Guillaume M., Herrera J., « LES MANIPULATIONS DE L'INFORMATION – Un défi pour nos démocraties », Rapport du Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères) et de l'Institut de recherche stratégique de l'École militaire (Irsem, Ministère des Armées), août 2018, [en ligne :] https://www.defense.gouv.fr/actualites/economie-et-technologie/lancement-du-rapport-conjoint-caps-irsem-les-manipulations-de-l-information, consulté le 21 avril 2020.

[134] Ripoche B., « États-Unis. Les deepfakes font encore plus peur que les fake news », Ouest France, 12/06/2019, [en ligne :] https://www.ouest-france.fr/monde/etats-unis/etats-unis-les-deepfakes-font-encore-plus-peur-que-les-fake news-6394487, consulté le 9 septembre 2020.

[135] La Defense Advanced Research Projects Agency (DARPA), (« Agence pour les projets de recherche avancée de défense ») est une agence du département de la Défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire.

[136] O'Sullivan D., « Quand voir n'est plus croire », CNN Business, 2016, [en ligne :] https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes, consulté le 21 avril 2020.

[137] Comme Tony Belpaeme : Professeur en IA et Robotique à l'Université de Gent ; Tom Lenaerts : spécialiste de l'IA, vice-président du département d'informatique de l'ULB, Président de l'Association Benelux pour l'IA et expert au sein du Global Partnership on AI, Georg Riekeles Directeur associé du European Policy Centre, Risto Uuk : Responsable de recherche pour l'UE au Future of Life Institute ; Cristina Vanberghen : Professeur Dr., EUI et Commission européenne, Reconnue par le Service européen pour l'action extérieure (SEAE) pour son rôle dans l'avancement de la diplomatie numérique dans le cadre du G20 et du G7, en particulier pour ses efforts dans la promotion de l'agenda numérique et cybernétique de l'UE en collaboration avec les pays partenaires ; Lode Lauwaert : Professeur de Philosophie de la technologie, KU Leuven ; Frederic Heymans : Chercheur au Knowledge Centre Data & Society ; Gianluca Bontempi : Professeur à l'ULB et fondateur du ULB Machine Learning Group …

[138] Critch A., « Disrupting the Deepfake Supply Chain », FAccT Conférence, le 21 février 2024, [en ligne :] https://openletter.net/l/disrupting-deepfakes, consulté le 5 août 2024.

[139] La rédaction de Security Hero, « 2023 state of deepfakes », Security Hero, 2023, [en ligne :] https://www.securityhero.io/state-of-deepfakes/, consulté le 10 août 2024.

[140] La rédaction d'Onfido, « Identity Fraud Report 2024 », Onfido, 2024, [en ligne :] https://onfido.com/landing/identity-fraud-report, consulté le 17 août 2024.

[141] Lettre ouverte, « Disrupting the Deepfake Supply Chain », FAccT Conférence, le 21 février 2024, *op. cit.*

[142] Poibeau T., « L'IA générative, un acteur majeur dans une société de la désinformation ? », The Conversation, le 7 mars 2024, [en ligne :] https://theconversation.com/lia-generative-un-acteur-majeur-dans-une-societe-de-la-desinformation-225051, consulté le 20 août 2024.

[143] La rédaction d'Evangéliques Info, « 665 millions d'évangéliques dans le monde en 2021 », Evangéliques Point Info, le 22 janvier 2021, [en ligne :] https://www.evangeliques.info/2021/01/22/665-millions-d-evangeliques-dans-le-monde-en-2021/, consulté le 17 septembre 2024.

[144] En 2022, l'organisation Christians United For Israel (Cufi) comptait 10 millions de membres.

[145] Lettre ouverte, « Disrupting the Deepfake Supply Chain », FAccT Conférence, le 21 février 2024, *op. cit.*

[146] David E., « No Fakes Act wants to protect actors and singers from unauthorized AI replicas », The Verge, le 12 octobre 2023, [en ligne :] https://www.theverge.com/2023/10/12/23914915/ai-replicas-likeness-law-no-fakes-copyright, consulté le 10 septembre 2024.

[147] La rédaction de l'Essentiel, « Les victimes de "deepfakes" porno se sentent démunies », l'Essentiel, le 13 septembre 2024 [en ligne :] https://www.lessentiel.lu/fr/story/en-coree-du-sud-les-victimes-de-deepfakes-porno-se-sentent-demunies-103184210, consulté le 17 septembre 2024.

[148] Un marquage aux données d'entraînement serait également imposé, pour savoir si des contenus ont été utilisés pour l'apprentissage de modèles de génération d'images, de textes…

[149] Lettre ouverte, « Disrupting the Deepfake Supply Chain », FAccT Conférence, le 21 février 2024, *op. cit.*

[150] El Attilah I., « La condamnation à perpétuité des victimes de "deepfake porn" », Euronews, le 30 juin 2023, [en ligne :] https://fr.euronews.com/next/2023/06/30/la-condamnation-a-perpetuite-des-victimes-de-deepfake-porn, consulté le 18 septembre 2024.

[151] Duboust O., « Deepfakes are spreading in scams and on social media 'faster than expected', experts warn », Euronews, le 13 juin 2024, [en ligne :] https://www.euronews.com/next/2024/06/13/deepfakes-are-spreading-in-scams-and-on-social-media-faster-than-expected-experts-warn, consulté le 15 septembre 2024.

[152] Sorte de tatouage numérique.

[153] La rédaction du Monde, « Les géants du numérique signent un accord contre l'utilisation trompeuse de l'IA dans le cadre d'élections », Le Monde, le 16 février 2024, [en ligne :] https://www.lemonde.fr/pixels/article/2024/02/16/les-geants-du-numerique-signent-un-accord-contre-l-utilisation-trompeuse-de-l-ia-dans-le-cadre-d-elections_6216967_4408996.html, consulté le 15 septembre 2024.

[154] La norme C2PA a été fondée en février 2021 par des leaders de l'industrie tels qu'Adobe, ARM, Intel, Microsoft, The New York Times et la BBC. Elle fonctionne en intégrant une métadonnée spécifique, considérée comme une signature numérique, dans les fichiers d'images générées par IA. Cette métadonnée fournit des informations clés sur l'origine de l'image et qu'elle a été produite par une IA.

[155] La rédaction du Monde, « Les géants du numérique signent un accord contre l'utilisation trompeuse de l'IA dans le cadre d'élections », *op. cit.*

[156] *Ibid.*

[157] Voir chapitre sur le Face Swapping.

[158] Meng Jing, « La Chine publie de nouvelles règles pour limiter les technologies de contrefaçon utilisées pour créer et diffuser de fausses nouvelles », South China Morning Post, 29 novembre 2019, [en ligne :] https://www.scmp.com/tech/apps-social/article/3039978/china-issues-new-rules-clamp-down-deepfake-technologies-used, consulté le 14 mai 2020.

[159] Commission Européenne, « The 2022 Code of Practice on Disinformation », Commission Européenne, mai 2021, [en ligne :] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation, consulté le 17 septembre 2024.

[160] Jacquet T., « Deepfakes pornographiques, politiques, économiques : quelles sont les sanctions prévues par le droit belge contre ces pratiques ? », *op. cit.*

[161] Suspension ou bannissement d'une plateforme.

[162] Grimonpont A., « Deepfakes : quatre solutions pour éviter la violation du droit à l'information », Rsf, le 29 février 2024, [en ligne :] https://rsf.org/fr/deepfakes-quatre-solutions-pour-%C3%A9viter-la-violation-du-droit-%C3%A0-l-information, consulté le 18 septembre 2024.

[163] Carbonaro G., « The AI detector tools that can help you check content for plagiarism, fakes and scams », Euronews, le 24 janvier 2024, [en ligne :] https://www.euronews.com/next/2024/01/24/plagiarism-fakes-and-copycats-these-are-the-best-tools-to-spot-ai-generated-content, consulté le 18 septembre 2024.

[164] Statistiques Statbel, « Pyramide des âges », Statbel, 2024, [en ligne :] https://statbel.fgov.be/fr/figures/pyramide-des-ages, consulté le 20 septembre 2024.

[165] Virtual Private Network pour Réseau Privé Virtuel, permettant une navigation privée.

[166] La rédaction du Courrier International, « Élections. "Deepfake", "cheapfake" : l'IA au service de la campagne présidentielle argentine », Courrier International, le 17 novembre 2023, [en ligne :] https://www.courrierinternational.com/article/elections-deepfake-cheapfake-l-ia-au-service-de-la-campagne-presidentielle-argentine, consulté le 20 septembre 2024.

Diplômée d'un master en Psychologie et d'un master 2 en Sociologie, Roxane Lejeune est collaboratrice dans la thématique Médias & Actions citoyennes chez Citoyenneté & Participation.

Toutes et tous devant les écrans

Quels effets pour la santé

Roxane Lejeune

Analyse

Introduction

Le dos et la nuque courbés, un rapetissement du cerveau, des bras en angle droit pour faciliter la prise d'un smartphone ou encore une deuxième paupière pour faire face à l'impact supposé de la lumière bleue de nos écrans sur nos yeux, telles seraient les évolutions corporelles prévues pour les humains dans mille ans, selon TollFree Forwarding, un opérateur de téléphonie[1]. En 2012 également une projection de l'être humain du futur le dotait d'un plus petit cerveau, car compensé par les ordinateurs[2].

L'omniprésence grandissante des écrans dans nos vies est certaine. Le nombre d'appareils connectés par foyer ne fait qu'augmenter. En Europe de l'ouest, le nombre moyen d'appareils connectés par personne était de 5,6 en 2018 et est passé à 9,4 en 2023[3]. Mais cette « course du tout au numérique » va-t-elle faire de nous des êtres difformes tels que le prévoient ces projections fantasques ? Probablement pas, mais ces dernières semblent mettre le doigt sur des inquiétudes et craintes partagées par nombre d'entre nous : nos écrans impacteraient notre santé.

Qu'en est-il réellement ? Avons-nous des raisons de nous inquiéter des conséquences que peuvent avoir nos compagnons tactiles sur notre santé ou tombons-nous plutôt dans une panique injustifiée ? L'objectif de cette analyse sera de revenir sur différents impacts supposés des écrans sur notre santé, souvent pointés par le public de nos animations d'éducation permanente, et de les analyser. Dans un premier temps, nous nous intéresserons aux effets directs et indirects des écrans, concernant notre santé physique et mentale. Dans un deuxième temps, nous questionnerons la notion « d'addiction aux écrans » souvent mobilisée par les publics que nous rencontrons dans nos ateliers d'éducation permanente, et entendue plus largement dans les discours médiatiques et quotidiens. Enfin, dans un troisième temps, nous discuterons des éléments sociaux et économiques liés à notre consommation contemporaine des écrans et, plus largement, du numérique.

1. Tous devant les écrans quelles conséquences pour notre santé ?

Myopie, cancer, obésité ou encore arthroses précoces, trouble du développement cognitif. De quoi avoir peur de nos écrans lorsqu'on s'intéresse vaguement à leurs impacts sur notre santé. Dans cette première partie, nous reviendrons brièvement sur les effets des écrans sur différents éléments de notre santé, souvent entendus dans nos ateliers d'éducation permanente. Il s'agira alors de peser le vrai du faux, le probable de la panique. Nous distinguerons les impacts directs, liés à l'appareil en tant que tel, des impacts indirects, plutôt liés aux contenus.

a. Effets directs des écrans

01. Lumière bleue, ennemie pour nos yeux et notre sommeil

Un des premiers effets souvent pointé du doigt est le développement des troubles de la vision, qui serait en partie provoqué par la lumière bleue fortement émise par nos écrans. Bien que ceux-ci l'émettent à des niveaux moins élevés que le soleil, la lumière bleue peut en effet entraîner de la fatigue oculaire lorsque l'exposition est prolongée[4].

Au-delà de cette fatigue oculaire, et éventuellement des migraines qui pourraient l'accompagner, il ne semble pas y avoir de consensus scientifique sur la toxicité à long terme pour nos yeux et notre vision[5]. En effet, si certaines études tendent à montrer une nocivité pour la rétine, pouvant amener des risques de développement d'une cataracte ou de dégénérescences maculaires[6], d'autres recherches relativisent ces résultats et concluent que l'usage domestique des lumières LED par exemple ne semble pas toxique pour la rétine[7].

De plus, de multiples interrogations apparaissent quant au lien entre développement de la myopie, de plus en plus répandue, et la surexposition aux écrans. De nombreux facteurs environnementaux, au-delà des risques génétiques et héréditaires existent. Parmi ceux-ci, par exemple, on retrouve la lecture fréquente et un large temps passé en intérieur exposé à une faible luminosité. Un lien entre la myopie et l'exposition aux écrans semble également apparaître. Cependant, les mécanismes à l'œuvre n'ont pas été identifiés, et seraient davantage liés à un mode de vie sédentaire et une période importante de temps passé en intérieur, sans exposition à la lumière naturelle, que suppose souvent l'utilisation d'écrans[8].

Par ailleurs, il est souvent rapporté que la lumière bleue naturellement émise par le soleil permet de réguler notre rythme circadien (notre rythme jour-nuit). Or, l'utilisation prolongée d'écrans émettant ces fameuses lumières bleues supprimerait la production de mélatonine, molécule sécrétée pas notre corps pour favoriser notre endormissement, amenant dès lors des perturbations du sommeil[9]. Ici également, les études se montrent prudentes. Certaines ne montrent pas de différences importantes dans le temps d'endormissement entre une population exposée à un écran avant le coucher et une population plongée dans la lecture d'un livre[10]. D'autres études montrent toutefois une corrélation importante entre l'exposition tardive des écrans chez les enfants (de six à seize ans) et la présence d'insomnie et d'hyperactivité[11]. Selon certaines de ces études comme par exemple celle publiée en 2019 par dix scientifiques et médecins, tous académiciens, dans le cadre d'une mission interministérielle en France sur les rapports entre l'enfant, l'adolescent, la famille et les écrans. Il y a été observé qu'une faible production de mélatonine provoquerait une désynchronisation de l'organisme entraînant des troubles du sommeil voire une fatigue chronique, des troubles de l'humeur et même de la dépression, des troubles de l'appétit, de la performance et de la vigilance[12]. Les chercheurs appellent « *les neurophysiologistes, les psychologues et les philosophes à travailler ensemble à la compréhension des relations homme-machines, afin de poser les bases éthiques des interactions susceptibles d'enrichir le registre des expressions et des interactions humaines, et de s'opposer à celles qui contribueraient à le réduire* ».

Le principe de vigilance doit prévaloir et ce sans oublier que nombre de chercheurs pointent également les arguments marketing faisant de la lumière bleue un risque oculaire important en vue de vendre des lunettes de protection anti-lumière bleue[13]. De fait, si certaines options sur les écrans d'ordinateur permettent un affichage plus confortable pour les yeux (l'affichage nocturne), et permettent ainsi de réduire le risque de fatigue oculaire, l'utilisation de lunettes spéciales contre la lumière bleue n'apporterait par contre aucune amélioration du sommeil ou une baisse de risques d'atteinte maculaire[14].

02. Les écrans et notre santé physique : obésité et problèmes squelettiques

Un des effets les plus documentés concernant l'exposition aux écrans est le développement de l'obésité. Ainsi, il apparaît que la surexposition aux écrans serait un facteur de risque de surpoids et de l'obésité chez les enfants et les adolescents[15].

La relation entre l'usage des écrans et l'obésité et le surpoids serait sous-tendue par quatre mécanismes. Premièrement, passer du temps devant les écrans encouragerait le grignotage et la prise calorique immédiate. Deuxièmement, cela amènerait à davantage d'exposition à la publicité pour des produits de mauvaise qualité nutritionnelle. Troisièmement, l'usage des écrans favoriserait un mode de vie sédentaire. Quatrièmement, un sommeil écourté et de moindre qualité, comme explicité ci-dessus, lié au développement de l'obésité, est également pointé du doigt[16]. Ces quatre mécanismes entrent d'ailleurs en interrelation chez certains jeunes qui, augmentant dès lors la surconsommation d'écrans, se sédentarisent, et l'amplifient encore davantage[17].

La surexposition aux écrans serait un facteur de risque de surpoids

Par ailleurs, il semblerait que l'usage de certains écrans soit également lié à l'apparition d'autres problèmes physiques, comme des troubles musculo-squelettiques. Par exemple, l'utilisation prolongée et répétitive d'écrans dans le milieu professionnel semble être liée au développement de douleurs dorsales, lombaires ou cervicales[18]. De même, les joueurs et joueuses excessifs de jeux vidéo semblent également être davantage exposés au risque de tendinite[19] ou de syndrome du canal carpien[20]. Si ces troubles musculo-squelettiques[21] peuvent se montrer inconfortables, ou douloureux, il semblerait toutefois qu'ils puissent être diminués par une meilleure posture, et par des pratiques ergonomiques.

03. Un cancer au bout du fil ?

Lors de nos animations d'éducation permanente, la crainte de l'apparition d'un cancer par l'utilisation excessive d'appareils numériques est parfois exprimée. Certaines participantes semblent ainsi préoccupées par l'impact des ondes émises par nos smartphones, par exemple. Qu'en est-il ?

Il n'y aurait à ce jour aucune donnée démontrant l'impact des champs électromagnétiques dans l'apparition de cancers[22]. Cette crainte fait écho à une des nombreuses inquiétudes adressées, notamment, à l'implémentation d'antennes 5G. Si certaines critiques peuvent effectivement être formulées, celle de l'apparition et du développement du cancer chez les utilisateurs et la population de manière générale n'est pas prouvée[23].

> Nous aurions également pu revenir sur différents éléments liés à la corrélation[24] entre la surexposition aux écrans chez les enfants et adolescents et un développement cognitif altéré. En effet, depuis de nombreuses années, nombre de chercheurs tirent la sonnette d'alarme et montrent de nombreuses relations entre l'exposition aux écrans et des troubles d'apprentissage du langage, de la mémoire, de l'attention, de la créativité, etc[25].
> Cependant, la littérature scientifique est prolifique à ce sujet, et a par ailleurs déjà été traitée par Citoyenneté & Participation en 2020. Nous vous renvoyons dès lors vers l'analyse complète sur le sujet réalisée par Karin Dubois[26].

b. Effets indirects des écrans

01. Violence et contenus non adaptés

Parmi les craintes et observations identifiées par les participants de nos ateliers concernant l'utilisation excessive des écrans, nous pouvons également citer la place importante de la violence, ou la présence de contenus non adaptés sur nos écrans et leur impact sur les plus jeunes.

La télévision et puis les jeux vidéo, sont souvent pointés du doigt, tant par des parents inquiets que parfois par des chefs d'état[27], comme pouvant rendre violents ses utilisateurs. Cependant, il semblerait que ce lien n'est pas aussi clair. D'après le psychiatre Serge Tisseron, « *les images ne rendent pas tous les enfants violents, mais elles peuvent rendre plus violents ceux qui ont tendance à l'être* »[28]. Par ailleurs, la question de la désensibilisation à la violence ou encore de la baisse d'empathie qui serait liée à la consommation de jeux vidéo violents est discutée et ne montre pas de consensus scientifique[29].

Cependant, il convient de préciser que les images violentes, intriquées dans un certain contexte, peuvent avoir des effets chez les plus petits, et ce d'autant plus lorsqu'elles représentent des évènements de la vie réelle[30][31]. S'ajoute à cela que pour les tout-petits, les mimiques et interactions avec les autres permettent de développer l'empathie émotionnelle. Le neuropsychiatre français Boris Cyrulnik affirme quant à lui que ce manque de synchronisation avec l'autre peut produire des adolescents qui ont du mal à contrôler leurs émotions[32].

Ainsi, il ne s'agit pas tellement du contenu violent en tant que tel qu'il faudrait pointer du doigt, mais davantage la possibilité qu'il puisse être consulté facilement par un jeune à un âge non adapté.

02. Dismorphophobie et perception du corps

L'utilisation des réseaux sociaux semble également liée au développement d'insatisfaction et une perception tronquée et négative du corps, tant chez les jeunes filles que chez les jeunes garçons[33].

En effet, la consultation de certains contenus, pro-anorexie sur TikTok par exemple amènerait chez certaines jeunes femmes et adolescentes une volonté de reproduire des standards de beauté mis en scène, une insatisfaction vis-à-vis de leur propre corps et potentiellement des risques de développer des troubles de conduites alimentaires (TCA), comme l'anorexie[34].

Les réseaux sociaux s'avèrent, par leur contenu, mettre en avant certains comportements et standards de beauté. Cependant, nos écrans ne seraient-ils pas des relais fourbes de problématiques sociales plus larges (comme l'hyper-sexualisation des corps féminins, l'installation de standards de beauté inatteignables, etc.) qui, certes sont mises en avant par nos réseaux sociaux (nous verrons dans le point III pourquoi), mais qui s'inscrivent dans notre société de manière générale ? Dès lors, nos écrans n'agissent-il pas comme des miroirs déformants reflétant notre réalité sociale et les problématiques qu'elle charrie ?

*

En conclusion de cette première partie consacrée à une brève revue de certaines craintes émises par les participants de nos animations en éducation permanente, il convient de revenir sur quelques éléments de réflexions.

Il est indéniable que l'apparition et l'omniprésence grandissante des écrans et appareils numériques dans nos vies quotidiennes a bouleversé notre rapport au monde, au point de questionner leurs effets sur notre santé et notre développement cognitif et psychologique. Ainsi, si la littérature scientifique et médicale s'est attachée à démontrer les différents risques liés à la surexposition aux écrans, surtout chez les plus jeunes, il convient cependant de se montrer prudents, et ne pas tomber pour autant dans un message alarmiste comme peuvent le sous-entendre certains médias.

En effet, une démarche scientifique rigoureuse est longue et conclure à une relation de causalité d'une variable (l'exposition des écrans par exemple) sur une autre (la qualité du sommeil, le développement du langage, etc. par exemple) n'est pas chose aisée. Nous vivons dans un monde complexe où nos vies sont

traversées par diverses influences et isoler l'une d'elle pour en démontrer l'impact net et certain est d'une grande complexité et demande de longues études longitudinales. Par exemple, comment démontrer clairement un lien entre l'exposition aux écrans et certains troubles sans prendre en compte nos modes de vie globalement sédentaires ? En d'autres termes, sommes-nous « malades » à cause des écrans directement ou plutôt parce que tout notre mode de vie est axé sur une moindre activité physique, une baisse globale du temps de sommeil, une moindre exposition à la lumière naturelle du soleil, etc. Autant d'éléments eux-mêmes corrélés à une meilleure santé ?

Dès lors, nous ne le rappellerons jamais assez : corrélation n'est pas causalité, et cela vaut également dans l'étude des effets que pourraient avoir nos écrans sur notre santé.

2. Toutes et tous addicts aux écrans[35] ?

Il n'est pas rare d'entendre, dans nos groupes d'éducation permanente, dans les médias, ou ailleurs, que l'addiction aux écrans est un fléau (et ce d'autant plus chez les jeunes). D'ailleurs, nous voyons fleurir de nombreux néologismes pour en rendre compte. Nombre de médias, nous parlent de la « *nomophobie* »[36] ou du « *fomo* »[37] comme « *la nouvelle maladie du siècle* »[38], comme « *une pathologie des temps modernes* »[39], comparant alors les écrans et les smartphones à de véritables drogues.

Des parents inquiets pour leurs enfants dévoreurs de contenus numériques, aux citoyens et médias préoccupés par l'omniprésence de l'influence des réseaux sociaux, le constat semble clair : les écrans et leurs contenus agissent comme des drogues. Mais qu'en est-il réellement ? Peut-on comparer notre nièce de treize ans fan de Valorant[40] et *likeuse* en série sur Instagram à une toxicomane en recherche de sa substance ? En d'autres termes, peut-on réellement parler d'addiction aux écrans ?

Aucun symptôme physiologique de sevrage ne semble avoir été démontré

Face à cette question deux camps s'opposent. Premièrement, l'approche naturaliste et biomédicale des addictions considère toute addiction comme une maladie, due au chamboulement neurophysiologique induit par la prise d'une substance psychotrope[41]. Dans ce modèle, on pourrait définir l'addiction comme une maladie issue d'une consommation excessive et problématique d'une ou de plusieurs substances psychoactives, amenant à une tolérance, du *craving*[42] et des symptômes de sevrage[43].

Ainsi, par exemple, si un alcoolique ou un héroïnomane est accro, c'est parce que l'alcool et l'héroïne sont des molécules qui, intrinsèquement par leurs actions physiologiques et neurologiques, vont avoir tendance à rendre addict les personnes qui en consomment excessivement, c'est-à-dire les amener à en consommer davantage pour ressentir les effets recherchés, à développer une recherche obsessionnelle et irrépressible du produit et à ressentir des « symptômes de manque » (qui peuvent parfois amener la mort, comme pour l'alcoolisme par exemple) lorsqu'il n'est pas possible de consommer.

Dans ce modèle, il semble évident que les addictions comportementales, comme la dépendance aux écrans, ne trouvent que peu leur place. En effet, selon cette approche, si certains peuvent avoir une consommation problématique des écrans, aucun symptôme physiologique de sevrage ne semble avoir été démontré lorsqu'une personne ne peut avoir sa « dose » d'écran[44].

Deuxièmement, une seconde approche de l'addiction existe, celle du modèle bio-psycho-social qui met davantage l'accent sur le contexte biologique, psychologique et social des individus dans leurs comportements de consommation et de leur éventuelle dépendance. L'addiction serait alors le produit d'une interaction complexe entre une génétique, une histoire personnelle, des besoins psychologiques, un contexte relationnel précis, etc. Dans cette conception, les addictions comportementales, telles que celle de la dépendance aux écrans, prennent leur place, puisqu'ici ce n'est pas tant le stimulus ou la substance addictogène qui est au centre des comportements d'addiction, mais bien le contexte dans lequel ceux-ci s'inscrivent. Ainsi, l'idée est de comprendre l'addiction comme une réponse à une motivation parfois inconsciente de l'individu (un mal-être psychologique, par exemple), suivant un désir d'évasion de la réalité, et non pas comme une conséquence presque mécaniciste d'une prise de substance[45].

Les grandes organisations de santé et de psychologie, comme l'OMS (Organisation mondiale de la Santé) et l'APA (American Psychological Association) et le consensus scientifique s'inscrivent aujourd'hui davantage dans la première approche des addictions. En effet, tant dans les classifications internationales comme la CIM ou le DSM, l'addiction aux écrans ou la dépendance à Internet ne sont pas reconnus[46], préférant parler d' « usage problématique des écrans ». Seule la classification internationale des maladies de l'OMS se voit complétée, en 2018, par le « trouble du jeu vidéo ». Celui-ci est défini comme :

> un comportement lié à la pratique des jeux vidéo ou des jeux numériques, qui se caractérise par une perte de contrôle sur le jeu, une priorité accrue accordée au jeu, au point que celui-ci prenne le pas sur d'autres centres d'intérêt et activités quotidiennes, et par la poursuite ou la pratique croissante du jeu en dépit de répercussions dommageables. [...] le comportement doit être d'une sévérité suffisante pour entraîner une altération non négligeable des activités personnelles, familiales, sociales, éducatives, professionnelles ou d'autres domaines importants du fonctionnement, et en principe, se manifester clairement sur une période d'au moins douze mois[47].

Or, ces grandes organisations médicales et leurs classifications ont tendance à donner le « la » et être sources de références pour nombre de communautés médicales. Ainsi, aux États-Unis par exemple, la reconnaissance des maladies et troubles reconnus par l'American Psychological Association, soumise à l'influence de lobbies pharmaceutiques, va faciliter la prescription de certains médicaments ou l'octroi de congés maladie[48], par exemple. En Europe, le corps médical et les assurances maladies tendent à s'appuyer sur les recommandations et la classification internationale des maladies de l'OMS[49].

Ainsi, la reconnaissance ou non d'un trouble, d'une maladie ou d'une addiction n'est pas anodine et répond à de nombreux rapports de force, qui impactent dès lors le secteur médical, les interventions, les traitements proposés mais également la recherche et les études statistiques.

Toutefois, au-delà des dictats de ces grandes organisations de santé, une réalité de terrain existe. Par exemple, en Belgique, plusieurs cliniques et services hospitaliers sont spécialisés dans la cyberdépendance au vu du nombre de personnes souffrant d'une consommation excessive et problématique des écrans (bien qu'elles soient surtout axées sur les jeux d'argent en ligne et le trouble du jeu vidéo, soit les deux addictions comportementales reconnues par l'OMS).

Finalement, si aucun consensus scientifique des grandes organisations de santé ne semble exister autour de la cyberdépendance mais qu'une certaine conception biopsychosociale de l'addiction aux écrans, ou « d'utilisation pathologique des écrans », peut être acceptée, il faudrait toutefois se montrer davantage prudent et ne pas tomber dans une panique morale. Si certaines personnes peuvent montrer des comportements « addictifs » avec les écrans, tout usage excessif n'est pas pour autant pathologique. À ce titre, la plupart des travailleurs du secteur tertiaire qui passent le plus clair de leur journée en face d'un ordinateur ne sont pas tous pour autant de grands addicts.

Par ailleurs, questionnons-nous sur ce que nous désignons instinctivement comme des comportements d'addiction aux écrans. En effet, n'avons-nous pas tendance à pointer comme addicts des jeunes lorsqu'ils jouent aux jeux-vidéos et consultent les réseaux sociaux, mais beaucoup moins lorsqu'ils doivent suivre leurs cours en ligne, ou faire leurs devoirs ? L'addict est celui qui consulte son smartphone dans le bus, poste des story Instagram, joue à League Of Legend en pyjama tous le week-end. Mais l'addict n'est pas le responsable RH face à ses tableaux Excel quotidiens, l'étudiante en pleines révisions, ou l'adolescent suivant ses cours en ligne durant un confinement suite à une épidémie mondiale. Pourquoi avons-nous ce réflexe de condamnation de l'usage excessif des écrans lorsqu'ils sont utilisés pour le divertissement et non pas lorsqu'ils répondent à des impératifs de productivité ?

Tout usage excessif n'est pas pour autant pathologique

3. À qui profite le crime ?

Un des premiers réflexes lorsqu'il s'agit de questionner l'impact des écrans sur notre santé et plus particulièrement celle des jeunes, est de pointer du doigt les parents et leurs mauvais principes d'éducation. Si nos chères têtes blondes deviennent des zombies obèses, déficients cognitifs, vulnérables aux tendinites et accro aux écrans, c'est bien à cause de ces parents indignes qui leur refilent leur smartphone en deux temps trois mouvements pour calmer leurs pleurs incontrôlables. Si probablement certains manquent de ressources, de temps ou d'informations quant aux risques associés aux écrans tels qu'on les a développés jusqu'ici, l'éducation parentale ne semble être que la pointe immergée de l'iceberg. D'ailleurs, cibler les parents comme l'unique origine de cette mauvaise utilisation numérique, au-delà de la culpabilisation induite, contribue également, inconsciemment ou non, à stigmatiser encore davantage les familles précaires, puisqu'on sait que les enfants auront tendance à être davantage exposés aux écrans précocement lorsqu'ils grandissent dans des familles issues de milieux socio-économiquement défavorisés[50].

Si nous passons notre temps à questionner les principes éducatifs des (« mauvais ») parents, et donc s'inscrire dans des critiques très individuelles où la conclusion serait « *formez-vous à être des meilleurs parents* »[51], nous perdons de vue toute l'organisation sociale, collective et économique qui nous amène à l'omniprésence des écrans dans notre vie quotidienne.

Pointons également les discours contradictoires, dans le chef des politiques publiques ou ailleurs, qui nous disent d'un côté de veiller à la santé et au développement des enfants face aux écrans, mais qui dans le même temps impulsent l'implémentation d'écrans dans le cadre scolaire[52] et poussent de plus en plus la population à utiliser des écrans, tant pour travailler, que pour faire des démarches administratives.

Ensuite, il convient de questionner les modèles économiques et sociaux qui sous-tendent notre utilisation des technologies numériques. En effet, notre manière d'utiliser notre smartphone, notre ordinateur portable ou encore notre console de jeu vidéo est soumise aux choix opérés par des entreprises privées qui n'ont pas forcément pour objectif notre santé et notre bien-être, comme semble le rappeler en 2017, Reed Hastings, le PDG de Netflix déclarant : « *nous sommes en concurrence avec le sommeil* »[53].

De fait, les GAFAM construisent leurs équipements et font des choix de développement et de production qui visent à nous vendre de plus en plus d'appareils numériques et puis à nous faire passer le plus de temps devant les écrans. Pourquoi ? Pour des raisons économiques, puisque au plus nous passons du temps sur les réseaux sociaux, Internet, des jeux en ligne, etc. plus nous laissons derrière nous des données personnelles, qui, une fois récupérées par ces entreprises (avec notre consentement), sont vendues à des *data-brokers* ou des entreprises privées, et ce, pour nous soumettre de la publicité ciblée[54]. Pour attirer notre attention et nous pousser à passer le plus de temps sur ces plateformes, plusieurs outils et stratégies existent, comme les algorithmes de recommandation, le *scroll* infini, la lecture automatique, les notifications intempestives, les « challenges » ou encore la mise en avant de contenus engageants[55]. C'est ce qu'on appelle l'économie de l'attention.

Tous ces exemples sont des choix[56]. Des choix opérés par les entreprises qui les développent et ce en vue de maximiser leurs profits. Dès lors, au-delà du fatalisme et des remises en question individuelles et familiales, un autre développement et une autre organisation du numérique, plus démocratique et plus soucieuse de nos besoins, est possible. Si nos modes de vie, notre psychologie et notre rapport au monde ont effectivement évolué au fil du développement technologique, que doit-on blâmer : la technologie en tant que telle ou la manière dont elle nous est imposée par des entreprises privées, elles-mêmes soumises aux lois du marché ?

Conclusion

En conclusion, la présence grandissante des écrans et des appareils connectés dans nos quotidiens n'est plus à démontrer. Leur omniprésence est telle que nombre de parents, citoyens, participants de nos animations d'éducation permanente, médias ou médecins s'inquiètent de leurs effets sur notre rapport au monde, mais également sur notre santé. L'objectif de cette publication était de revenir sur ceux-ci et d'en discuter les contours, et ce pour éveiller notre œil critique sans prendre le risque de tomber dans une panique morale.

Dans un premier temps, nous sommes revenus sur les différents effets directs et indirects du numérique sur notre santé, souvent évoqués sur le terrain de l'éducation permanente et ailleurs. Dans un deuxième temps, nous nous sommes attardés sur la notion, difficile à aborder, d'« addiction aux écrans ». Enfin, dans un troisième temps, une réflexion plus large a été amorcée à propos des enjeux sociaux et économiques derrière l'omniprésence du numérique et de leur possible impact sur notre santé.

Finalement, par cette analyse, l'idée est de questionner les différents poncifs, les réflexes assertifs et les inquiétudes que nous pouvons avoir face à la numérisation grandissante de nos vies. Au regard de ce qui a été discuté, il semblerait nécessaire de relativiser mais également de se montrer prudents. Notre rapport au monde et nos comportements professionnels, scolaires, sociaux changent au rythme des progrès technologiques et de nombreuses paniques et critiques peuvent apparaître, et le numérique n'y échappe pas. Il convient donc de se méfier : qu'est-ce qui est l'objet de critique ? L'appareil et la technologie en tant que telle, ou bien les raisons qui amènent sa généralisation, la manière dont elle nous est imposée ou comment nous sommes poussés à l'utiliser ?

D'ailleurs, loin de nous l'idée de renier les avantages indéniables du numérique dans nos vies et pour notre santé. En effet, nous aurions pu évoquer dans cette analyse le soutien numérique pour les personnes en situation de handicap, ou encore dans la prévention et le suivi médical pour certaines maladies mentales ou physiques, comme le suivi de sa glycémie pour les personnes atteintes de diabète ou l'aide à la détection de certains cancers, par exemple.

Quoi qu'il en soit, de nombreuses critiques de la numérisation à outrance de nos vies peuvent malgré tout être émises, et ce cahier s'attache à en expliciter certaines. De cette manière, au travers de ces riches et diverses réflexions, questionnements et échanges du terrain, un autre horizon peut être aperçu, celui d'un numérique davantage axé sur les (non-)besoins, le bien-être et l'égalité des utilisateurs (par exemple, dans l'accessibilité, l'utilité et l'attention aux usages de chacun)[57]. Et cet autre numérique ne peut s'opérer qu'au travers d'une organisation collective, citoyenne et fondamentalement démocratique, en dehors des logiques de marché imposées par les GAFAM, BATX et autres NATU.

[1] « À quoi pourrait ressembler l'être humain en l'an 3000 ? Une société a développé un modèle », La Libre, 09 novembre 2022, [en ligne :] https://www.lalibre.be/lifestyle/magazine/2022/11/09/a-quoi-pourrait-ressembler-letre-humain-en-lan-3000-une-societe-a-developpe-un-modele-4NPNSNV3PBGUPKOWLVH6WDCQIY, consulté le 28 août 2024.

[2] Vanlerberghe C. « À quoi ressemblera l'homme dans 1000 ans ? », Le Figaro, 12 octobre 2012, [en ligne :] https://www.lefigaro.fr/sciences/2012/10/12/01008-20121012ARTFIG00487--quoi-ressemblera-l-homme-dans-1000-ans.php, consulté le 28 août 2024.

[3] « Cisco Annual Internet Report (2018–2023) White Paper », Cisco, 09 mars 2020, [en ligne:] https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, consulté le 05 septembre 2024.

[4] « La lumière bleue : Est-elle nocive ? », Association canadienne des optométristes, 11 mai 2023, [en ligne :] https://opto.ca/fr/bibliotheque-sante-oculovisuelle/la-lumiere-bleue-est-elle-nocive, consulté le 02 septembre 2024.

[5] Stroili M., « Lumière bleue : est-elle réellement dangereuse pour nos yeux ? », Rtbf, 03 mai 2024, [en ligne :] https://www.rtbf.be/article/lumiere-bleue-est-elle-reellement-dangereuse-pour-nos-yeux-11368222, consulté le 02 septembre 2024

[6] Renard G. et Leid J., « Les dangers de la lumière bleue : la vérité ! », mai 2016, Journal français d'ophtalmologie, 5, vol. 39, pp.483-488 [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S0181551216300018, consulté le 02 septembre 2024.

[7] Cougnard-Gregoire A. et coll., « Blue Light Exposure: Ocular Hazards and Prevention – A Narrative Review », 18 février 2023, Ophtalmology and Therapy, vol. 12, pp.755-788, [en ligne :] https://link.springer.com/article/10.1007/s40123-023-00675-3, consulté le 02 septembre 2024.

[8] « Peut-on devenir myope à cause d'une exposition aux écrans », Futura-Science, 1 mai 2023, [en ligne :] https://www.futura-sciences.com/sante/questions-reponses/corps-humain-peut-on-devenir-myope-cause-exposition-ecrans-17943, consulté le 18 octobre 2024.

[9] « La lumière bleue : Est-elle nocive ? », *op. cit.*

[10] Chang A-M. et coll., « Evening use of light-emitting eReaders negatively affects sleep, circadian timing, and next-morning alertness », Proceedings of the National Academy of Sciences, 4, vol.112, pp.1232-1237.

[11] Chaussoy L. et coll., « Les écrans influencent le comportement des enfants par le biais d'une perturbation du sommeil », Médecine du Sommeil, mars 2019, 1, Vol. 16, p.62, [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S1769449319301232, consulté le 03 septembre 2024.

[12] Ades J. *et al.*, L'enfant, l'adolescent, la famille et les écrans, Mildeca Mission interministérielle de lutte contre les drogues et les conduites addictives. Publication du rapport, 16 avril 2024, [en ligne :] https://www.drogues.gouv.fr/publication-du-rapport-lenfant-ladolescent-la-famille-et-les-ecrans, consulté le 9 septembre 2024.

[13] Mainste A. et coll., « The Blue Light Hazard Versus Blue Light Hype », American Journal of Ophtalmology, août 2022, Vol.240, pp.51-57, [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S0002939422000721, consulté le 02 septembre 2024.

[14] Lawrence J., Hull C. et Downie L., « The effect of blue-light blocking spectacle lenses on visual performance, macular health and the sleep-wake cycle: a systematic review of the literature », Ophtalmic Physiol Opt, novembre 2017, 6, vol.37, pp.644-654, [en ligne :] https://pubmed.ncbi.nlm.nih.gov/29044670, consulté le 02 septembre 2024.

[15] Fang K., Mu M., Liu K. et He Y., « Screen time and childhood overweight/obesity: A systematic review and meta-analysis », Child : care, health and development, septembre 2019, 5, vol. 45, pp.744-753, [en ligne :] https://onlinelibrary.wiley.com/doi/abs/10.1111/cch.12701, consulté le 03 septembre 2024.

[16] Courbet D. et Fourquet-Courbet M-P., « Usages des écrans, surpoids et obésité », Obésité, octobre 2019, 3, vol.14, pp.131-138, [en ligne :] https://www.researchgate.net/publication/336355464_Usages_des_ecrans_surpoids_et_obesite, consulté le 03 septembre 2024.

[17] *Ibid.*

[18] Zomalhéto Z., Ayelo A., Lawin H. et Fayomi B. « Les troubles musculo-squelettiques liés au travail sur écran d'ordinateur en milieu professionnel au Benin », janvier 2015, Revue Internationales des Sciences Médicales, 3, vol.17, pp.114-117, [en ligne :] https://www.researchgate.net/publication/297716493_MUSCULOSKELETAL_DISORDERS_RELATED_TO_WORK_ON_A_COMPUTER_SCREEN_IN_THE_WORKPLACE_IN_BENIN, consulté le 04 septembre 2024.

[19] Henry C. « La "tendinite de la console", vous connaissez ? », Ouest France, 07 mai 2018, [en ligne :] https://www.ouest-france.fr/sante/la-tendinite-de-la-console-vous-connaissez-5746647, consulté le 04 septembre 2024.

[20] Boy L. « "J'ai mal rien que d'y repenser" : pour les joueurs de e-sport, les blessures n'ont rien de virtuel », France Info, 19 mars 2018, [en ligne :] https://www.francetvinfo.fr/culture/jouets/j-ai-mal-rien-que-d-y-repenser-pour-les-joueurs-de-e-sport-les-blessures-n-ont-rien-de-virtuel_2589644.html, consulté le 04 septembre 2024.

[21] Fouquet B. et Herisson C., Syndrome du canal carpien et travail sur écran, Neuropathologies et pathologies professionnelles, n°59, 2007, pp.94-100, [en ligne :] https://portaildocumentaire.inrs.fr/Default/doc/SYRACUSE/140630/syndrome-du-canal-carpien-et-travail-sur-ecran-extrait-de-fouquet-b-ed-herisson-c-ed-et-coll-neuropa?_lg=fr-FR, consulté le 9 septembre 2024.

[22] « Potential health effects of exposure to electromagnetic fields (EMF) », Commission européenne, 27 janvier 2015, [en ligne :] https://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_041.pdf, consulté le 02 septembre 2024.

[23] « Effets de la 5G sur la santé », Parlement européen, juillet 2021, [en ligne :] https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690012/EPRS_STU(2021)690012_FR.pdf, consulté le 02 septembre 2024.

[24] Guez A. et Ramus F. « Les écrans ont-ils un effet causal sur le développement cognitif des enfants ? », Revue suisse de pédagogie spécialisée, avril 2019, 4, vol.9, pp.14-21, [en ligne :] https://ojs.szh.ch/revue/article/view/99, consulté le 30 août 2024.

[25] Par exemple voir : Harlé B. et Desmurget M., « Effets de l'exposition chronique aux écrans sur le développement cognitif de l'enfant », Archives de Pédiatrie, 7, vol.19, juillet 2012, pp.772-776, [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S0929693X12001947, consulté le 30 août 2024.

[26] Dubois K., « Quand les écrans sabotent l'apprentissage et impactent le développement des enfants. Le nouveau fléau des familles », 2020, Citoyenneté & Participation, Analyse n° 410, [en ligne :] http://www.cpcp.be/publications/ecrans-developpement-enfants.

[27] Telling M., « Macron voit un lien entre jeux vidéo et émeutes, mais "scientifiquement, c'est faux" », Huffpost, 01 juillet 2023, [en ligne :] https://www.huffingtonpost.fr/life/article/macron-voit-un-lien-entre-jeux-video-et-emeutes-mais-scientifiquement-c-est-faux_220008.html, consulté 30 août 2024.

[28] Dubé C., « Les écrans rendent-ils violent ? », Québec Science, 30 juillet 2010, [en ligne :] https://www.quebecscience.qc.ca/societe/les-ecrans-rendent-ils-violent, consulté le 30 août 2024.

[29] Lengersdorff L., « Neuroimaging and behavioral evidence that violent video games exert no negative effect on human empathy for pain and emotional reactivity to violence », novembre 2017, eLife, [en ligne :] https://elifesciences.org/articles/84951#s2, consulté le 29 août 2024.

[30] Tisseron S., « L'enfant au risque des médias », Enfances & Psy, 2005, 26, vol.1, pp.15-22, [en ligne :] https://shs.cairn.info/revue-enfances-et-psy-2005-1-page-15?lang=fr, consulté le 29 août 2024.

[31] *Ibid.*

[32] Dubois K., *op. cit.*

[33] Revranche M., Biscond M. et Husky M., « Lien entre usage des réseaux sociaux et image corporelle chez les adolescents : une revue systématique de la littérature », avril 2022, L'encéphale, 2, vol.48, pp.206-218, [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S0013700621002189, consulté le 29 août 2024.

[34] Blackburn M. et Hogg R., « #ForYou? the impact of pro-ana TikTok content on body image dissatisfaction and internalisation of societal beauty standards », Plos One, 7 août 2024, [en ligne :] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0307597, consulté le 29 août 2024.

[35] Le sujet de l'addiction aux écrans a déjà été abordé dans le cadre d'une analyse par Citoyenneté & Participation en 2018. Le sujet étant toujours aussi central dans nos ateliers d'éducation permanente, surtout lorsque nous échangeons avec des parents, il s'agit ici d'une brève remise en perspective amenant à de nouvelles réflexions. Voir : Streel M., « Surexposition aux écrans. Une nouvelle addiction juvénile », Citoyenneté & Participation, 2018, analyse n°352, [en ligne :] http://www.cpcp.be/publications/addiction-ecrans.

[36] Il s'agit de l'anxiété ressentie lorsqu'on est séparé de son smartphone.

[37] Il s'agit de l'acronyme pour « Fear of missing out » (comprenez « avoir peur de passer à côté de quelque chose »).

[38] « La nomophobie, c'est grave docteur ? », Le Soir, 17 mai 2017, [en ligne :] https://www.lesoir.be/art/1504806/article/soirmag/soir-mag-sante/2017-05-17/nomophobie-c-est-grave-docteur, consulté le 24 juillet 2024.

[39] *Ibid.*

[40] Il s'agit d'un jeu vidéo multijoueur de tir à la première personne.

[41] Un psychotrope est une substance qui induit des changements de perceptions, de sensations, d'humeur ou de conscience. Certains psychotropes sont considérés comme plus addictifs ou plus toxiques que d'autres. Ainsi, l'alcool, le LSD, le tabac ou encore le café sont des psychotropes, par exemple, mais tous n'amènent pas forcément de dépendance ou au même niveau de toxicité.

[42] Il s'agit de l'envie irrépressible de consommer une substance psychoactive, parfois jusqu'à l'obsession et amenant une recherche compulsive du produit.

[43] Ogden J., « Les comportements de dépendance », Psychologie de la santé, 2014, Louvain-La-Neuve : De Boeck Supérieur, pp.83-118.

[44] Tisseron S., « L'enfant et les écrans : un avis de l'Académie des Sciences », Le carnet Psy, 2013, 169, vol.2, [en ligne :] https://shs.cairn.info/revue-le-carnet-psy-2013-2-page-1?lang=fr, consulté le 26 juillet 2024.

[45] Trouessin M., « L'addiction aux écrans existe-t-elle ? », 2016, Séminaire IMPEC, [en ligne :] https://www.researchgate.net/profile/Melanie-Trouessin/publication/303677881_L'addiction_aux_ecrans_existe-t-elle/links/574c8b7a08aec9885269e27d/Laddiction-aux-ecrans-existe-t-elle.pdf, consulté le 26 juillet 2024.

[46] Notez que dans le DSM-V, seul le jeu d'argent est considéré dans les addictions comportementales.

[47] Notez qu'il n'y a malgré tout pas de consensus scientifique sur le sujet. « Trouble du jeu vidéo », Organisation mondiale de la Santé, 22 octobre 2020, [en ligne :] https://www.who.int/fr/news-room/questions-and-answers/item/gaming-disorder, consulté le 25 juillet 2024.

[48] Voir Frances A., « An insider's revolt against out-of-control psychiatric diagnosis, DSM-5, Big Pharma, and the medicalization of ordinary life », 2013, William Morrow & Co.

[49] « L'addiction aux jeux vidéo reconnue comme maladie par l'OMS », RTBF, 19 juin 2018, [en ligne :] https://www.rtbf.be/article/l-addiction-aux-jeux-video-reconnue-comme-maladie-par-l-oms-9949219, consulté le 25 juillet 2024.

[50] Kabali H. et coll., « Exposure and Use of Mobile Media Devices by Young Children », Pediatrics, décembre 2015, 6, vol.136, [en ligne :] https://pubmed.ncbi.nlm.nih.gov/26527548/, consulté le 19 août 2024.

Voir aussi : Dore R. et Dynia J., « Prevalence and Predictors of Background Television Among Infants and Toddlers from Low-Income Homes », Infant Behavior and Development, août 2021, vol.64, [en ligne :] https://www.sciencedirect.com/science/article/abs/pii/S0163638321000928, consulté le 19 août 2024.

[51] Notons qu'aider les parents à accompagner leurs enfants dans leurs usages du numérique est primordial, tant nombre d'entre eux se sentent dépassés par les évolutions technologiques et numériques.

[52] Même si l'usage des smartphones est aujourd'hui interdit dans l'enceinte des écoles officielles, on peut par exemple citer le plan « école numérique » de Digital Wallonia : https://www.digitalwallonia.be/fr/publications/ecole-numerique-2022-2026-actions/.

[53] Cassely J.-L., « Le vrai concurrent de Netflix ? Votre sommeil », Slate, 19 avril 2017, [en ligne :] https://www.slate.fr/story/144029/vrai-concurrent-netlfix-sommeil, consulté le 20 août 2024.

[54] Abiteboul S. et Cattan J., « Nous sommes les réseaux sociaux », 2022, Odile Jacob.

[55] Voir Socialter, « Peut-on échapper à l'emprise du numérique », juin-juillet 2024, n°64.

[56] La série de vidéo « Dopamine » d'Arte démontre parfaitement tous les mécanismes développés pour chaque réseau social afin de nous faire passer le plus de temps dessus.

[57] Il s'agit de remettre au centre du développement numérique et de leur implémentation dans différents secteurs de la société les usages, le bien-être et les besoins de chacun. Par exemple, d'autres critères, au-delà de la recherche de profits, pourraient être mis en avant, comme par exemple l'accessibilité, l'utilité pour les citoyens, la sécurité ou la santé psychologique et physique des utilisateurs.

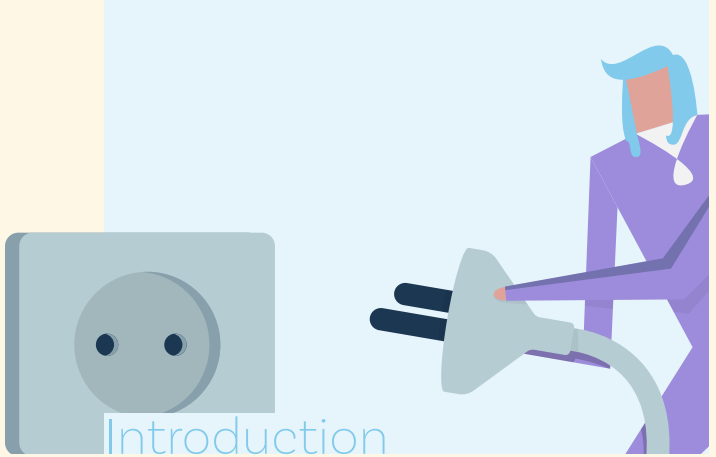
Anna Constantinidis est titulaire d'un doctorat en langues et lettres. Elle est chargée de recherche pour la thématique Médias & Actions citoyennes au sein du pôle Recherche & Plaidoyer et formatrice chez Citoyenneté & Participation.

La sobriété numérique

Au-delà des idées reçues

Anna Constantinidis

Étude



Introduction

Avant d'écrire cet article, nous avons interrogé de manière informelle plusieurs personnes autour de nous (collègues, ami·e·s, participant·e·s à des ateliers Médias organisés par notre association) sur les termes ou idées qui leur venaient à l'esprit lorsqu'on évoquait l'expression « sobriété numérique ». Voici les réponses qui sont majoritairement ressorties : écolo, truc de bobo, colibri, déconnexion, tri des mails, moins de vidéos. La sobriété numérique semble passer, dans le chef de nombreuses personnes (et pour nous aussi, avant de nous intéresser davantage au sujet), pour un horizon individuel impliquant une réduction de nos usages d'internet. Et allant de pair, de facto, avec une culpabilisation, ce qui peut bien sûr être mal perçu, à tel point qu'on ne veuille même pas entendre parler du sujet. Or la sobriété numérique, dans son acception scientifique, est bien plus un horizon collectif, sociétal, qu'une démarche individuelle. Naturellement, une forme de sobriété numérique peut relever de choix personnels, que l'on pose pour des raisons d'écologie, de santé, d'hygiène de vie ; néanmoins, on verra que ceux-ci : premièrement, ne sont pas toujours adéquats (la sobriété numérique charrie avec elle de nombreuses fausses bonnes idées, souvent issues du greenwashing) ; deuxièmement, sont plus difficilement tenables s'ils sont posés de manière isolée et, troisièmement, auront peu d'impact s'ils ne sont pas soutenus par des politiques publiques qui vont dans ce sens[1].

Pourquoi la sobriété numérique est-elle souhaitable ?

Cette publication a donc pour objectif, d'une part, de faire mieux connaître la réalité qui se cache derrière le concept de sobriété numérique, en évitant les écueils ; d'autre part, de proposer un plaidoyer pour un avenir sobre numériquement. Isabelle Autissier, présidente de WWF France, dans la préface d'un livre de Frédéric Bordage (fondateur de Green IT France et spécialiste de la sobriété numérique), explique : « *Le numérique n'est ni bon ni mauvais. C'est une technologie inventée par l'humanité […]. Comme tout progrès technologique, il sera ce que les hommes en feront : le pire ou le meilleur, un terreau fertile pour nos enfants ou une fuite en avant vers une catastrophe annoncée* »[2]. Le but de la sobriété numérique, on le verra, n'est pas de remettre en question l'existence du numérique, mais au contraire d'apprendre à en tirer le meilleur tout en respectant les limites planétaires.

Dans ce cahier, nous avons analysé un certain nombre d'enjeux et de risques collectifs liés à ce que nous avons nommé la « course au tout-au-numérique » : fracture et inaccessibilités, enjeux démocratiques du numérique, problèmes de santé et de santé mentale liés à une surutilisation des écrans, impacts du développement des smartcities et de la numérisation du recrutement, impacts écologiques du numérique, surveillance et business des données personnelles. Le choix de ces sujets ne signifie pas pour autant que l'équipe Médias de Citoyenneté & Participation est technophobe ; nous avons conscience des nombreux apports positifs du numérique[3], mais il nous semble important de nous pencher sur ces problématiques qui touchent tous les citoyen·ne·s et d'interpeller nos lecteurs et lectrices sur ces sujets démocratiques de premier plan. Après avoir pointé un certain nombre de problèmes, il nous a paru pertinent de proposer, comme dernier texte de ce cahier, un article sur les solutions possibles. Car, comme le dit Alain Damasio, « *une authentique technocritique ne peut se contenter d'être réactionnaire ou négative. Elle doit aussi esquisser ce que serait une technologie positivement vécue* »[4]. C'est donc sur le seul horizon tenable car écologiquement viable, mais aussi, sans doute, le plus sain pour la société et les individus, que nous avons décidé d'écrire : l'horizon de la sobriété numérique.

Dans ce parcours de (re)découverte, la première partie abordera une question simple : pourquoi la sobriété numérique est-elle souhaitable, voire indispensable, sur un plan environnemental ? Sera ensuite exploré, au point deux, ce qui se cache derrière celle-ci : qu'est-ce que la sobriété numérique, et quels sont les différents scénarios de sobriété possibles ? Dans la troisième partie, il sera question de la situation actuelle en Belgique, en particulier en Wallonie : la sobriété fait-elle l'objet d'une attention de la part du monde politique ? Quelles sont les forces en présence ? Le quatrième chapitre abordera quelques mesures politiques qui pourraient être mises en place pour tendre vers une forme de sobriété numérique, à différents niveaux : pour les citoyens et citoyennes, pour les entreprises, au niveau de la production, aussi. Enfin, on terminera par une réflexion globale sur la place des technologies numériques dans notre société et dans nos vies, et sur ce que pourrait nous apporter une société décroissante en la matière. Y seront évoquées la démarche low-tech ainsi que quelques-unes des recommandations formulées par Alain Damasio dans son dernier livre, Vallée du Silicium[5]. Afin d'alimenter les réflexions contenues dans cette étude, trois entretiens ont été menés : avec Olivier Vergeynst, directeur de l'Institut Belge du Numérique Responsable (ISIT-BE), avec Louise Marée, responsable

du programme DigitalWallonia4Circular de l'Agence wallonne du numérique (AdN), et avec David Bol, professeur en Circuits et Systèmes électroniques à l'École polytechnique de l'UCLouvain. Nous leur adressons ici nos remerciements les plus chaleureux pour le temps qu'ils nous ont consacré et les précieuses réponses apportées à nos questions[6].

Notre souhait est que cette étude puisse devenir un temps d'arrêt, accessible à toutes et tous car non technique, pour prendre du recul face à un sujet extrêmement clivant où on peut entendre, en tant que citoyen·ne, tout et son contraire : comment s'y retrouver en effet entre les plaidoyers contre le tout-au-numérique et le discours ambiant qui vante les effets de la numérisation de la société ? Entre les rapports qui affirment que la situation actuelle est intenable et ceux, soutenus par l'industrie technologique et repris par certaines personnalités politiques, qui assurent que le numérique « nous sauvera » ?[7] Un temps d'arrêt qui est tout sauf anodin, car « s'arrêter, c'est résister », nous rappelle le biologiste Olivier Hamant, que nous aimons à citer dans nos articles et qui, dans son dernier essai, insiste sur ce point : « *pour transformer réellement, nous dit-il, c'est-à-dire muter, il faut d'abord s'arrêter* »[8]. Cela semble évident, mais en réalité, l'arrêt, poursuit-il, « *est un geste révolutionnaire dans un monde en pleine accélération* »[9]. C'est dans cet esprit que se place notre travail, qui invite à un temps de pause afin d'encourager des réflexions individuelles et collectives sur la possibilité de la sobriété numérique.

1. Pourquoi la sobriété numérique ?

La sobriété numérique est, selon les spécialistes qui s'occupent de la question, la seule voie possible pour assurer l'avenir du numérique, et cette affirmation repose sur un constat : il s'agit d'« *une ressource cruciale mais limitée* »[10]. Nous ne donnerons ici que quelques chiffres-phares en vrac, à même de plus marquer les esprits que de longs discours :

- On évalue l'impact du numérique en termes de gaz à effet de serre, au niveau mondial, entre 2 et 4% des émissions, « *soit plus que l'aviation civile* »[11].
- « *À l'horizon 2050, si rien n'est fait, l'empreinte carbone du numérique pourrait tripler entre 2020 et 2050* »[12], voire quadrupler dans certaines projections, « *du fait notamment de l'explosion du nombre d'objets connectés, du volume de données et du développement des centres de données* »[13]. Vu les développements récents de l'intelligence artificielle (IA) et les investissements massifs dans ce domaine, on peut facilement se figurer les scénarios les plus pessimistes en termes d'empreinte carbone et d'autres impacts environnementaux[14].
- En France, l'ADEME (Agence française de la transition écologique) estime que « *62,5 millions de tonnes de ressources sont consommées pour la fabrication et l'utilisation des appareils numériques* »[15].
- La consommation électrique du numérique correspond à 5 à 8% de la consommation au niveau mondial : « dit autrement, si l'usage du numérique était un pays, il serait le troisième plus grand consommateur d'électricité au monde, juste après la Chine et les USA »[16].
- Le nombre d'objets connectés devrait dépasser quarante-cinq milliards d'ici 2030[17].
- On compte 5,3 milliards d'utilisateurs d'internet au niveau mondial ; 50 000 Go de données enregistrées[18].
- La production de smartphones à l'échelle mondiale entre 2008 et 2018 a été de 10,3 milliards, ce qui signifie qu'on a multiplié la production par onze en l'espace de dix ans[19].
- Dans un ménage standard (en France, donc on peut étendre à l'Europe), on compte entre quinze et quarante-cinq appareils numériques[20]. Et le recyclage de ces appareils est une chimère : « *sur les 70 métaux contenus dans un smartphone par exemple, seuls 5 seront récupérés* »[21].

Mais le plus inquiétant, comme le dit Frédéric Bordage, c'est « *la vitesse à laquelle cet univers grandit* »[22], d'autant plus depuis l'arrivée de l'Intelligence Artificielle.

Si on ne prend « que » la question environnementale en compte, il est pourtant évident, indique le collectif AlterNumeris (collectif belge réunissant des chercheurs et chercheuses de différents horizons réfléchissant aux enjeux de la société numérique)[23], que le numérique a « *un impact direct négatif incontesté* »[24]. Et il s'agit là non seulement des émissions de gaz à effet de serre, donc de la question du dérèglement climatique (à laquelle sont souvent restreints, à tort, les impacts du numérique sur l'environnement), mais de tous les critères permettant de savoir si l'humanité dépasse les limites planétaires, à savoir « *14 catégories d'impact environnementaux ainsi que leurs indicateurs associés* »[25] définies par l'Union européenne, parmi lesquelles : « l'*épuisement des ressources abiotiques, l'acidification, l'écotoxicité des eaux douces, les radiations ionisantes […]* »[26]. À ces faits s'ajoutent des problèmes sociaux et démocratiques (fracture et accessibilité numérique, risques démocratiques, impacts sanitaires non négligeables). Malgré cela, la numérisation « à tous les étages », pour reprendre une expression du collectif[27], est souvent présentée comme le seul

horizon possible et envisageable par nombre de discours politiques. Au niveau européen, d'ailleurs, les transitions numérique et écologique sont articulées, alors qu'elles sont, en réalité, en contradiction[28].

Pourtant, une autre voie est possible, qui semble d'ailleurs, selon nombre de spécialistes, la seule issue possible : celle « *d'un numérique piloté, qui sait choisir ses directions : au vu des opportunités, mais également au vu des risques* »[29], autrement dit, la sobriété numérique.

2. Qu'est-ce que la sobriété numérique ?

La sobriété numérique, « *c'est passer d'un numérique instinctif, voire compulsif, à un numérique piloté* »[30]. Pour ce faire, elle est avant tout une prise de conscience, et un questionnement des besoins.

a. Une prise de conscience des impacts environnementaux du numérique

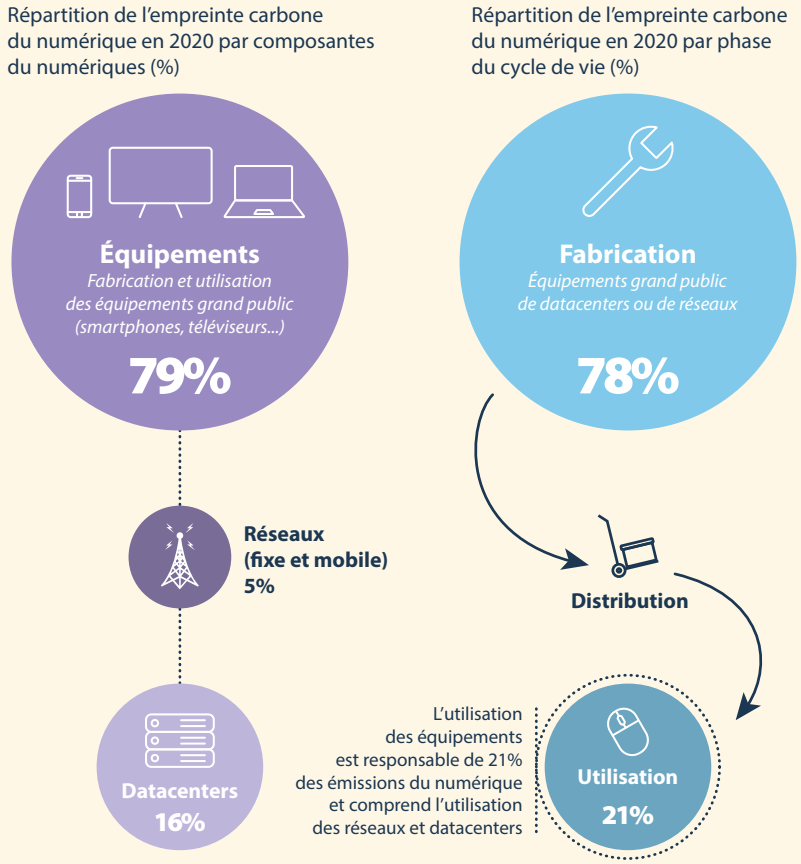
On l'a vu en introduction, le terme « sobriété » peut rebuter car il est associé à la privation (pensons surtout à la consommation d'alcool). Or, la sobriété est littéralement la « tempérance dans le boire et le manger », « la mesure », « la modération »[31]. Pour éviter ce terme qu'on associe donc erronément à une privation, Olivier Vergeynst, directeur de l'Institut Belge du Numérique Responsable (ISIT Belgique), lui préfère celui de « modération numérique ». La dénomination est différente, mais l'idée est la même : c'est utiliser le numérique, mais l'utiliser à bon escient[32]. Et pour ce faire, c'est avant tout prendre conscience des impacts environnementaux liés à son utilisation[33]. Parmi ceux-ci, nous ne prendrons ici que l'aspect climatique en question (qui est donc partiel, comme on l'a vu plus haut, mais qui est un bon moyen d'expliquer intelligiblement le fait que le numérique est tout sauf immatériel).

Dans ce cadre, on identifie généralement l'impact des équipements et celui des usages :

- Les équipements peuvent être répartis en trois catégories : les centres de données (data centers), les réseaux de transmission des données (antennes 4G, par exemple) et les terminaux des utilisateurs·trices (smartphones, ordinateurs portables ou non, consoles, écrans, box TV, imprimantes, compteurs intelligents, montres connectées ou autres objets connectés, clés USB et disques durs externes, autres terminaux utilisés dans les habitations).
- Les usages (stockage de données sur le cloud, visionnage de vidéos, etc.), qui impliquent surtout de la consommation électrique, mais sont aussi liés aux équipements réseaux (« plus on consomme de données, plus on va avoir besoin d'antennes 4G, 5G pour transmettre ces données, de data centers pour les stocker, etc.) »[34], et aux équipements 'utilisateurs' : si on a des usages moins gourmands, on n'aura peut-être pas besoin du smartphone dernier cri le plus élaboré, mais d'un modèle reconditionné plus modeste ; par ailleurs, les objets dureront forcément plus longtemps s'il y a davantage de modération dans leur utilisation.

Pour les équipements : les impacts vont s'identifier sur leurs trois phases de vie : fabrication, utilisation, fin de vie. Les rapports sur le sujet se rejoignent sur le constat que les impacts les plus importants sont liés à la phase de fabrication, suivie de celle des usages. En termes de pourcentages : « *entre 70 à 85% pour la fabrication (70 pour laptop, 85 pour smartphones), puis l'impact en termes d'électricité dans la phase des usages (essentiellement pour les data centers)* », nous rappelle Olivier Vergeynst[35]. Si on ne prend que l'empreinte carbone en considération, l'ADEME[36] nous indique qu'en 2020, 78 % de celle-ci était due à la phase de fabrication, pour les trois types d'équipements (équipements grand public, centres de données et réseaux), puis à l'utilisation. Dans les trois types d'équipements, ce sont les terminaux des utilisateurs·trices qui sont les plus impactants : 79 % de l'empreinte carbone totale, contre 5 % pour les réseaux, et 16 % pour les centres de données[37]:

L'empreinte carbone du numérique dépend essentiellement des équipements et de leur fabrication



Source : https://www.arcep.fr/la-regulation/grands-dossiers-thematiques-transverses/lempreinte-environnementale-du-numerique/etude-ademe-arcep-empreinte-environnemental-numerique-2020-2030-2050.html, consulté le 11 juin 2024.

Alors que certains (rares) rapports nous disent que le numérique va permettre d'améliorer notre impact sur l'environnement d'ici quelques années (comme le rapport Digital4Climate, commandité il y a deux ans par Agoria, le lobby du secteur technologique en Belgique)[38], deux éléments sont indéniables selon le collectif AlterNumeris, qui réunit des experts indépendants, universitaires et du monde de l'IT :

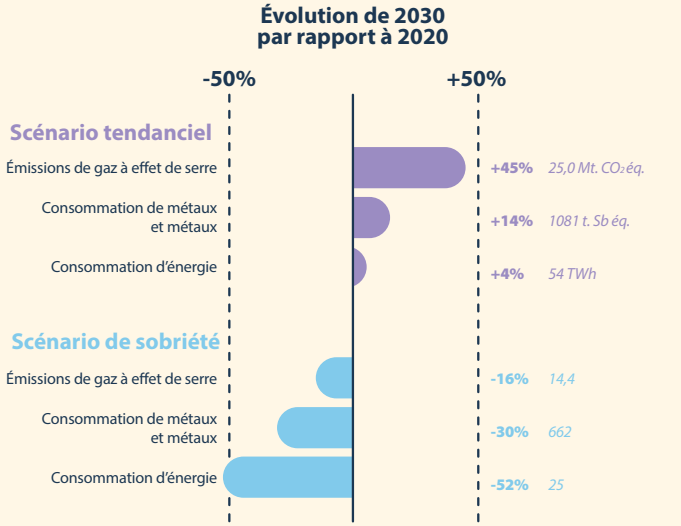
- En l'absence de certitude et de données quantifiables sur les effets positifs qu'il pourrait amener, le principe de précaution devrait toujours s'appliquer. C'est pourquoi le collectif invite à « *adopter le réflexe des trois regards (expert, politique, citoyen) dès qu'une nouvelle connaissance est produite* »[39] dans le domaine (cf. infra).
- On peut discuter de certains chiffres, mais il évident, comme on l'a déjà dit, que le numérique « a un impact direct négatif » incontestable sur l'environnement : « *L'extraction, la production, l'utilisation et la fin de vie des équipements physiques permettant les services digitaux ont un impact direct négatif considérable sur la planète. Il s'agit donc de reconnaître enfin le couple numérique/environnement comme un problème d'intérêt général* »[40].

Et cet impact, si l'on continue sur notre lancée, est voué à se démultiplier au vu du développement des objets connectés, des villes connectées, de la 5G, de l'IA, de l'internet par satellites version Musk[41], dans un processus qui semble inéluctable. Or, cette tendance n'est pas impossible à arrêter. Selon l'ADEME, on a un levier d'action : celui de tendre vers des politiques de sobriété numérique : « *des politiques […] qui commencent par une interrogation sur l'ampleur du développement de nouveaux produits ou services numériques et une réduction ou stabilisation du nombre d'équipements. L'allongement de la durée de vie des terminaux, en développant davantage le reconditionnement et la réparation des*

équipements est un axe majeur de travail, tout comme la sensibilisation des consommateurs à ces enjeux. De la même manière, afin d'améliorer notamment l'efficacité énergétique, l'écoconception doit être systématisée : pour les terminaux, mais aussi pour l'ensemble des équipements (infrastructures de réseaux et centres de données), ainsi que dans le cadre des modalités de déploiement des réseaux et services numériques. La mise en œuvre de l'ensemble de ces leviers permettrait de réduire l'empreinte environnementale du numérique d'ici à 2030 : jusqu'à -16% pour l'empreinte carbone par rapport à 2020 »[42]. Le schéma suivant est très parlant :

La combinaison de mesures de sobriété et d'écoconception permettrait de réduire l'impact environnementaldu numérique

Évolution des trois principaux critères (sur tout le cycle de vie) de l'impact environnemental du numérique en 2030, comparés à 2020, selon la poursuite des tendances actuelles ou l'application d'actions de sobriété.



Source : https://presse.ademe.fr/2023/03/impact-environnemental-du-numerique-en-2030-et-2050-lademe-et-larcep-publient-une-evaluation-prospective.html, consulté le 11 juin 2024.

On retrouve dans l'argumentaire développé par l'ADEME les trois plans d'actions donnés par Frédéric Bordage dans un de ses livres sur la sobriété numérique :

- diminuer la quantité d'équipements
- améliorer la durabilité
- et faire en sorte que l'usage des solutions numériques soit « *réellement utile aux individus et à la société* »[43].

Cela nous amène à ce qui devrait devenir une boussole pour toute décision concernant la numérisation, au niveau collectif mais aussi au niveau individuel : le questionnement des besoins.

b. Un questionnement des besoins

Sur le plan de l'information, il importe surtout, nous a expliqué Olivier Vergeynst, de déconstruire les fausses bonnes idées liées au numérique durable, où le greenwashing est légion, et d'informer sur les vrais impacts de taille : « *Le vrai enjeu dans les campagnes de sensibilisation, c'est de donner les ordres de grandeur pour que les gens se focalisent sur les grandes actions. Il y a des milliers d'actions, mais pour le grand public, il faut se focaliser sur les gros gains pour ne pas s'éparpiller. Et là, les trois axes prioritaires sont : 1) questionner le besoin ; 2) si besoin il y a vraiment, acheter du reconditionné plutôt que du neuf ; 3) donner une vraie deuxième vie aux objets, car comme pour d'autres secteurs, le recyclage est la dernière solution, sachant que sur les 70 métaux contenus dans un smartphone par exemple, seuls 17 peuvent être recyclés et seuls 5 le seront réellement, souvent avec un taux de perte important à chaque cycle* »[44]. Pour les structures, il s'agit également de promouvoir l'écoconception des applications, outils, etc.[45] Le questionnement des besoins est central. Louise Marée, responsable du programme DigitalWallonia4Circular à l'Agence du Numérique, le souligne également : « *Je n'utilise pas le mot 'sobriété', qui fait peur, mais par contre, quand on parle de numérique responsable, il faut qu'une solution soit utile, utilisable et utilisée, et derrière ça, il y a la sobriété aussi : on en revient toujours à questionner le besoin* »[46].

Ces questionnements ne peuvent naître si des politiques de sensibilisation et d'information sur les impacts du numérique ne sont pas mises en place, et si par ailleurs, les institutions publiques ne montrent pas l'exemple. Ainsi, si les seuls mots que nous entendons en tant que citoyen·ne·s sont la « nécessaire digitalisation des villes, des administrations », la « simplification administrative via le numérique », « l'indispensable développement de l'IA », comment pourrons-nous nous interroger sur les impacts de nos usages ? Par ailleurs, une administration aura plus de poids pour demander aux structures répondant à des appels à projets de répondre à des critères de durabilité si elle suit elle-même les critères en question ; ainsi d'une école, d'une association, etc.

La sobriété numérique, en somme, ce n'est pas suivre tel ou tel conseil, poser tel ou tel geste. C'est pourquoi cet article ne se veut pas une liste de recommandations individuelles. La sobriété numérique, indique le Shift Project, « *c'est piloter [...] les déploiements d'infrastructures et d'usages associés afin de préserver les apports essentiels du numérique* »[47]. Ce pilotage des usages va inévitablement de pair, selon nous, avec la question de quel numérique nous voulons : celui qui est développé par des mastodontes de type GAFAM, qui se pensent au-dessus des lois (même si l'UE, heureusement, tente désormais de les réguler) et qui développent des produits addictifs basés sur l'économie de l'attention, nos failles cognitives et le business des données personnelles ? Ou un numérique construit différemment, éthique, décentralisé, pensé démocratiquement comme une alternative aux GAFAM et autres BATX[48] ?

Enfin, il nous semble important de garder un autre aspect à l'esprit : pour ne pas que la sobriété numérique soit vécue comme une privation, il faudra pouvoir identifier, collectivement, ce que la société et chaque individu qui la compose a à gagner dans un scénario d'avenir moins connecté : outre bien sûr la diminution des impacts sur l'environnement, quels effets de telles politiques auraient-elles en termes de tissu social, de relations humaines ; en termes de santé, de santé mentale, d'égalité et de justice sociale. La réflexion sur la sobriété numérique ne peut donc se développer que main dans la main avec une réflexion sur les autres futurs possibles. À ce sujet, ces mots d'Alain Damasio résonnent en nous depuis plusieurs mois : « Il faut battre le techno-capitalisme sur le terrain du désir »[49]…

3. Quelle sobriété numérique ?

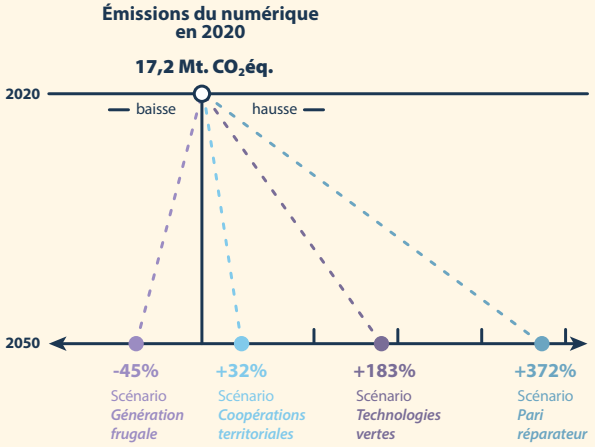
Il existe différents types de sobriété, en fonction d'où on place le curseur. Dans une étude prospective de l'ADEME intitulée « Transitions 2050 », quatre scénarios (désormais « S1, S2, S3 et S4 ») ont été envisagés à l'horizon 2050 pour atteindre la neutralité carbone en France : (S1) génération frugale, (S2) coopérations territoriales, (S3) technologies vertes, (S4) pari réparateur. Ces scénarios « *empruntent des voies distinctes et correspondent à des choix de société différents* »[50]. Dans chacun de ceux-ci est envisagée une articulation spécifique entre numérique et environnement.

a. Génération frugale (S1) ou Coopérations territoriales (S2)

Parmi les quatre scénarios, seuls les deux premiers, « *misant sur des politiques de sobriété numérique ou d'écoconception (comme S1 et S2), montrent qu'il existe des pistes d'action permettant de décarboner sensiblement le secteur du numérique* »[51]. Alors que dans le scénario 1, l'empreinte carbone pourrait être divisée par trois, dans les S3 et S4 (à savoir technologies vertes et pari réparateur), accrochons-nous : « *l'empreinte carbone pourrait tripler dans le scénario tendanciel par rapport à 2020, voire quadrupler ou plus dans S4, du fait notamment de l'explosion du nombre d'objets connectés, du volume de données et du développement des centres de données* »[52].

Choix de société : une empreinte carbone quintuplée ou divisée par deux d'ici 2050

Taux d'évolution des quatre scénarios prospectifs d'émissions de CO_2éq. du numérique en 2050 (sur tout le cycle de vie) par rapport à 2020 de l'étude ADEME-Arcep.



Source : https://presse.ademe.fr/2023/03/impact-environnemental-du-numerique-en-2030-et-2050-lademe-et-larcep-publient-une-evaluation-prospective.html, consulté le 11 juin 2024.

Le visuel montre que le seul scénario permettant de diminuer les émissions actuelles de CO_2 est le premier, avec une diminution nette (-45 %) d'ici 2050. Comme le résume AlterNumeris dans le rapport « *Faire cohabiter numérique et environnement ?* », *où sont explorés ces scénarios prospectifs, ce scénario est celui d'« une sobriété radicale et une transformation rapide des modes de vie* »[53], où les maîtres-mots seraient : low-tech, réparation, mutualisation, collaboration, stabilisation des flux. « *La numérisation du monde doit être limitée, contrainte et exclusivement réservée aux usages répondant aux besoins fondamentaux ou garantissant un impact neutre sur l'environnement* »[54]. Le scénario 2 associe quant à lui sobriété et efficacité dans « *un équilibre progressif et négocié* » : nous nous faisons à l'idée que si sobriété il y a un jour, c'est ce scénario qui apparaît plus réaliste, au moins dans un premier temps, avant de bifurquer vers le premier lorsque l'on sera au pied du mur… Dans le scénario 2, on retrouve surtout du IT for green, c'est-à-dire que « *la technologie sert à suivre les impacts fondamentaux des transformations conduites. Elle se focalise sur la prévention des risques naturels et la production de solutions fondées sur l'ingénierie écologique* »[55]. Voici un schéma réduit dans lequel nous avons choisi trois éléments du schéma original : les grandes lignes de ce que serait la société dans chaque horizon, de ce que serait la technique, et de ce que serait la gouvernance :

	S1 GÉNÉRATION FRUGALE	S2 COOPÉRATIONS TERRITORIALES	S3 TECHNOLOGIES VERTES	S4 PARI RÉPARATEUR
Société	• Recherche de sens • **Frugalité choisie mais aussi contrainte** • Préférence pour le local • Nature sanctuarisée	• Évolution soutenable des modes de vie • **Économie du partage** • Équité • Préservation de la nature inscrite dans le droit	• **Plus de nouvelles technologies que de sobriété** • Consumétisme « vert » au profit des populations solvables, société connectée • Les services rendus par la nature sont optimisés	• Sauvegarde des modes de vie de **consommation de masse** • La nature est une ressource à exploiter • Confiance dans la capacité à réparer les dégâts causés aux écosystèmes
[...]				
Technique Rapport au progrès, numérique, R&D	• Innovation autant organisationnelle que technique • **Règne des low-tech**, réutilisation et réparation • Numérique collaboratif • **Consommation des data centers stable** grâce à la stabilisation des flux	• Investissement massif (efficacité énergétique, EnR et infrastructure) • Numérique au service du développement territorial • **Consommation des data centers stable** grâce à la stabilisation des flux	• Ciblage sur les **technologies les plus compétitives pour décarboner** • Numérique au service de l'optimisation • Les data centers consomment 10 fois plus d'énergie qu'en 2020	• Innovations tout azimut • Captage, stockage ou usage du carbone capté indispensable • Internet des objets et AI omniprésents : les **data centers consomment 15 fois plus d'énergie** qu'en 2020
Gouvernance Échelle de décision, coopération internationale	• **Décision locale**, faible coopération internationale • Réglementation, interdiction et rationnement via des quotas	• Gouvernance partagée • **Fiscalité environnementale** et redistribution • Décisions nationales et coopération européenne	• Cadre de **régulation minimale** pour les acteurs privés • État planificateur • Fiscalité carbone ciblée	• Soutien de l'offre • Coopération intenationale forte et ciblée sur quelques filières clés • **Planification centralisée du système énergétique**

Partie du tableau de synthèse des scénarios prospectifs de l'ADEME, sous-parties « société », « technique » et « gouvernance » [56].

b. Les imaginaires d'AlterNumeris

Il nous semble intéressant de relier ici[57] ces scénarios prospectifs de l'ADEME aux imaginaires qui gravitent autour du numérique évoqués par AlterNumeris dans un rapport sur la 5G rédigé en 2021 : La 5G au-delà du pour ou contre (auteurs Jérémy Grosman, Julien Raone et Steve Tumson, ainsi que plusieurs contributeurs).

Pour AlterNumeris, il est essentiel de développer des imaginaires liés au développement technique, car cela permet de politiser une technologie : « *manquer cette étape, c'est prendre un développement technique par le petit bout de la lorgnette, c'est négliger ce qui se joue au-delà de ses usages et ses enjeux* »[58].

Trois imaginaires sont développés (de manière schématique) pour montrer les différentes « conceptions du monde en présence » : (1) le techno-capitalisme, (2) la social-démocratie et (3) l'éco-socialisme.

Voici la partie du tableau dédiée à la technologie numérique. Ci-dessous, dans la colonne 1, le scénario techno-capitaliste ; dans la colonne 2, la social-démocratie ; dans la troisième colonne, l'éco-socialisme.

(3) Technologie numérique			
Niveau de gestion des outils numériques (Qui prends les décisions ?)	Décision technicienne ; centralisation de la gestion et décentralisation de la collecte de données via objets connectés	Décisions aux représentants ; centralisation de la gestion et de la collecte des données	Décision aux utilisateurs ; décentralisation de la gestion et de la collecte de données
Périmètre de technologie (Quelle place pour les technologies numériques ?)	Monde des objets connectés ; tous les faits et gestes de la vie quotidienne sont ponctués en données ; maîtrise humaine de la nature	Le recours est encadré par des régulations ; technologies numériques d'utilité publique ; détermination de secteurs prioritaires et de secteurs protégés	Le numérique est limité au strict nécessaire ; les technologies sont accédées dans les limites du milieu de vie et des ressources disponibles
Valeurs cardinales (Quelles valeurs président aux rapports avec le numérique ?)	*The sky is the limit* ; ce qui est possible doit être réalisé ; tout ce qui entrave le développement de la technologie va à l'encontre de l'intérêt général	Pluralisme technologique, recherche d'un équilibre entre technologies individualisées, communautaires et transcommunautaires ; respect des droits fondamentaux	Autolimitation ; la technologie comme moyen de libérer le temps ; les ressources disponibles doivent orienter le choix technologiques ; la recherche de l'autonomie
Conception de la technologie (Quelle représentation prévaut ?)	Solution universelle à tous le problèmes modernes, en ce compris écologique	Équilibrée et délibérée ménageant les intérêts sociaux et économiques	*Small, low, slow tech* ; sobriété ; le numérique en dernier recours

Rapport AlterNumeris, La 5G au-delà du pour ou contre, p. 32, téléchargeable à l'adresse https://www.alternumeris.org/la-5g-au-dela-du-pour-ou-contre/

La sobriété numérique, en fonction de ce qu'on entend par là (sobriété radicale ou équilibre entre sobriété et efficacité, à savoir les scénarios 1 et 2 de l'ADEME), se situerait donc ici dans la colonne 3 (sobriété radicale) ou 2 (sobriété/efficacité). Le lecteur intéressé pourra compléter ces tableaux par la lecture de la partie « Les programmes d'action publique » du rapport « Faire cohabiter numérique et environnement ? », où les auteurs développent des exemples de leviers-phare pour les programmes techno-capitaliste, social-démocrate et de sobriété radicale[59].

Ces scénarios gagneraient d'après nous à être davantage connus du grand public et à être démocratisés, par exemple via des actions d'éducation permanente : ils pourraient alors percoler dans des groupes de réflexion citoyens, afin de recueillir les avis de la population sur ceux-ci, et de voir si le premier scénario, qui est actuellement celui qu'on dessine pour notre société, recueille l'adhésion, ou pas…

4. Où en est-on en Wallonie ?

Rappelons, en amont de ce paragraphe, 1) que les politiques de transformation numérique, notamment la digitalisation des services publics, s'insèrent dans la double transition européenne évoquée plus haut[60] ; 2) que l'orientation donnée s'intègre dans une vision positive du numérique[61], une vision qui prévaut encore largement en Belgique, même si, on va le voir, les choses sont peut-être en train de changer.

a. Quelle connaissance des impacts ?

Si l'on s'en tient simplement à la connaissance des impacts environnementaux, il semble que la Belgique, il y a encore peu de temps, n'était pas très « avancée ». Pour tester cette impression, nous avons sollicité l'avis expert d'Olivier Vergeynst : « *Oui, la Belgique est certainement en retard sur ces questions. À la base, personnellement je viens du monde de l'IT et je baigne dans l'informatique depuis mes six ans, or jusqu'il y a six ou sept ans, je n'imaginais pas du tout les impacts dont on parle. Je me suis donc dit que si moi je n'étais pas au courant, les autres ne devaient pas l'être non plus. J'ai donc été me former en France sur ces questions car la France était beaucoup plus avancée sur le sujet : un écosystème y existe déjà depuis longtemps. C'est sur le modèle de l'INR en France que j'ai créé l'Institut du Numérique Responsable Belge, en 2020* »[62]. Entre autres explications, le désintérêt des pouvoirs publics pour ces questions, donc l'absence, pendant longtemps, de rapports et d'études documentant ces impacts[63].

Force est de constater en effet que la quantité de sources scientifiques sur ces impacts est limitée et récente, alors qu'on trouve nombre de publications françaises, par exemple, et depuis longtemps, sur les liens entre numérique et environnement (Ademe, Shift Project, Green IT, Les Amis de la Terre, etc.). En Belgique, il y a un an, on ne recensait, comme nous l'a confirmé Olivier Vergeynst, que trois études d'ensemble :

- Un rapport de Climact[64] demandé par le gouvernement wallon dans le cadre de travaux parlementaires, mais dont les chiffres ne sont pas publics, nous a expliqué Olivier Vergeynst[65] ; un autre travail de Climact, accessible quant à lui, concernant la consommation d'électricité liée au numérique en Wallonie (2021)[66] ;
- Un rapport sur les liens entre numérique et environnement commandité par Agoria, l'organisation professionnelle de l'industrie technologique en Belgique et intitulé Digital4Climate[67](le titre dit bien l'orientation qui y est donnée…). Un rapport qui a été pris pour référence par plusieurs de nos dirigeant.e.s politiques, alors même qu'il était clairement biaisé[68], ce qui avait déjà été relevé par un journaliste à l'époque concernant l'absence de prise en compte des effets rebond et de l'épuisement des ressources[69], et qui a été prouvé par A+B dans le rapport de février 2024 d'AlterNumeris[70].
- Une étude rédigée par l'Agence du numérique wallonne à la demande du ministre de l'Économie et du Numérique, sur « Numérique et environnement »[71], où on trouve un résumé des constats dressé sur un ensemble de sources, dans la partie 1, « Principaux constats »[72].

Aujourd'hui, on peut aussi compter sur l'excellent rapport (cité plus haut) *Faire cohabiter numérique et environnement ?* d'AlterNumeris (auteurs Steve Tumson, Julien Raone, Miguel Coma, membres du collectif, ainsi que de nombreux contributeurs) publié en février 2024, et sur sa méthodologie des trois regards, relayée par le site internet de la stratégie wallonne Digital Wallonia[73]. Dans ce rapport, le collectif émet deux principales recommandations :

- « *adopter le réflexe des trois regards dès qu'une nouvelle connaissance est produite dans le domaine* ». Cela permettra d'éviter que des rapports tels que celui du lobby Agoria précité soient pris pour référence par des politiques dans la sphère publique : « *En effet, l'application des 3 regards sur la dernière étude belge en date (Digital4Climate) suggère que la reprise de cette étude dans un contexte de décision politique serait inappropriée, voire contre-productive pour l'environnement* » ;
- « *Dans l'incertitude, appliquer le principe de précaution* » : […] « *chaque secteur économique doit travailler à la réduction de son empreinte écologique, sans exception pour le numérique* »[74].

Le collectif, par la politisation de la société numérique qu'il entend opérer et grâce à la qualité de ses publications et interventions, va certainement faire bouger les lignes.

b. La stratégie numérique wallonne

Pour mieux comprendre si les impacts environnementaux du numérique sont pris en compte dans l'orientation digitale donnée à la Wallonie, nous avons parcouru le site de Digital Wallonia, la stratégie pour la Wallonie numérique, portée par l'Agence du numérique[75]. Un surf rapide sur le site permet de découvrir les programmes de la stratégie et d'aisément imaginer la volonté de développer le digital dans tous les domaines ou presque : Agriculture du Futur, DigitalWallonia4.Business, DigitalWallonia4.Edu, DigitalWallonia4.Startups, GigaRegion, DigitalWallonia4.Citizens, DigitalWallonia4.IA, Leadership numérique, etc.[76] L'agence du numérique nous a toutefois indiqué que dans cette stratégie numérique, la question de l'environnement a été intégrée dès 2015 comme un enjeu transversal, plusieurs programmes ayant intégré des actions dans ce domaine. Actuellement, cette thématique est néanmoins principalement adressée au travers du programme DigitalWallonia4Circular, visant surtout l'utilisation du numérique pour développer l'économie circulaire en Wallonie. Ce programme, comme nous l'a expliqué sa responsable, Louise Marée, a débuté assez récemment (fin 2022-début 2023) et se situe à mi-chemin entre les stratégies Wallonie digitale et Wallonie circulaire : « *DigitalWallonia4Circular vise notamment à développer un secteur numérique en faveur d'une économie plus verte et plus résiliente et aussi de l'économie circulaire : c'est une optique du numérique au service de l'économie circulaire dans d'autres secteurs que le numérique* », en considérant le numérique comme un outil et non comme une finalité. Ceci à travers la mise en relation des acteurs de l'économie circulaire avec les porteurs de solutions numériques, avec de la sensibilisation, des missions de veille, des appels à projets, une cartographie de l'économie circulaire, etc.[77] : le lecteur curieux d'en savoir plus trouvera une synthèse très intéressante de tous les projets portés par ce programme dans le Livre Blanc de DigitalWallonia4Circular, publié en juillet 2024[78].

Pour l'instant, la stratégie, comme l'indique son nom, a donc été beaucoup plus axée sur l'IT for Green, à savoir l'utilisation du numérique pour diminuer l'empreinte environnementale d'autres secteurs, que sur le Green IT ou le « numérique vert », durable. Néanmoins, les porteurs du programme ont pour souhait d'intégrer de plus en plus le Green IT dans leur stratégie, comme nous l'a indiqué Louise Marée, et comme le montre le Livre Blanc précité : dans ses éclairages préliminaires, cette étude rappelle les cinq grands constats ayant émergé de l'étude de 2021 sur Numérique et Environnement (cf. supra) : « *la prise en compte de l'ensemble du*

cycle de vie des outils numériques » ; « *les avancées numériques ne sont pas sans conséquence* » ; « *les avancées numériques peuvent également représenter des opportunités* » ; « *attention aux effets rebond* » et « *les modes de comportement au centre de tout* »[79]. Le livre blanc reprend également une des recommandations de l'étude d'AlterNumeris : « *face à l'incapacité d'affirmer clairement si le numérique réduit l'empreinte écologique globale, chaque secteur, y compris le numérique, devrait s'efforcer de diminuer son impact environnemental* »[80]. Louise Marée nous l'a confirmé lors de notre entretien : « *Je pense que la question des impacts environnementaux du numérique gagne progressivement en visibilité. Autrefois, il était plus courant de se concentrer principalement sur le numérique au service de la circularité, mais on constate désormais une plus grande ouverture à la discussion sur le Green IT. Il semble qu'il y ait davantage de liberté pour sensibiliser sur ces enjeux. J'ai bon espoir que, quelles que soient les politiques qui suivront la stratégie actuelle, les enjeux environnementaux du numérique seront de plus en plus pris en considération* »[81]. L'intégration du Green IT nous semble en effet cruciale. Comme nous l'a expliqué David Bol, professeur en Circuits et Systèmes électroniques à l'École polytechnique de l'UCLouvain, lors de notre entretien : « *Les nombreux usages en IT4Green ne dispensent pas du GreenIT, ça ne dispense pas de limiter les impacts directs du numérique […], car on ne peut pas faire l'amalgame de dire que parce qu'il y a des effets positifs, ils sont plus importants que les effets négatifs, et qu'il faut d'abord développer le numérique, puis en dégager les usages pertinents… ça me semble trop spéculatif comme position, et ça met toujours les autres secteurs non numériques dans une position plus difficile en termes d'impacts environnementaux : si on laisse le numérique partir en termes de GES, il y a en effet moins de place pour les autres secteurs* »[82].

Numérique responsable et sobriété numérique ne sont pas équivalents

À ce propos, notons que la Déclaration de politique régionale 2024-2029 va dans le sens d'une intégration plus forte du Green IT avec l'IT for Green pour minimiser l'impact environnemental des technologies, mais par ailleurs, celle-ci reste clairement sur les rails – et les accentue – de ce qu'on a appelé plus haut le scénario techno-capitaliste : déploiement de la 5G, connectivité, intelligence artificielle, transformation des entreprises, développement des compétences numériques, digitalisation de l'administration[83]. Même si l'environnement est de plus en plus pris en compte dans les stratégies numériques, on l'a vu, la sobriété numérique semble encore lointaine. Pourtant, nous croyons dur comme fer qu'il faudra y passer : reste à voir si ce sera volontaire ou si nous y serons contraints.

c. Tour d'horizon

Par rapport à la démarche de numérique responsable, Olivier Vergeynst nous a expliqué qu'à la Région Bruxelloise, ces questions commencent à se frayer un chemin : la Région se fait en effet accompagner par l'Institut Belge du Numérique Responsable, dans une démarche d'exemplarité. Par ailleurs, de plus en plus d'appels à projets intègrent des questions liées à la gestion du numérique dans leurs formulaires, un aspect appelé à se renforcer[84].

Au Fédéral par contre, Agoria, le lobby belge des industries technologiques, a beaucoup de poids, nous a expliqué Olivier Vergeynst. On trouve peu d'intérêt pour les questions de durabilité numérique et, par conséquent encore moins pour la sobriété. Par ailleurs, il faut aussi prendre en compte une différence culturelle entre la Wallonie et la Flandre à ce sujet : « *D'une part car du côté francophone, on est plus informé de ce qui se passe en France ; d'autre part car la réalité culturelle et économique est différente en Flandre, où l'aspect durable de l'IT au niveau des entreprises est moins pris en compte : on le remarque car la consultance numérique responsable n'a pas réussi à percer dans le domaine flamand, ou très peu* »[85].

Un espoir cependant : la création de l'Institut Belge du Numérique Responsable en 2020 a marqué un tournant en Belgique[86]. Numérique responsable et sobriété numérique ne sont pas équivalents, mais le fait que la Belgique soit dotée d'une structure comme celle-là, qui puisse accompagner les administrations, entreprises, associations, dans une transition vers un numérique plus durable, est une avancée notable dans la bonne direction. Ainsi que nous l'a expliqué Olivier Vergeynst, la démarche de l'Institut se divise en quatre volets, dont les deux principaux sont : comment réduire l'impact environnemental du numérique et comment améliorer l'accessibilité des services[87]. Par son travail, l'Institut montre qu'une transition vers un numérique responsable est dans l'intérêt de ceux qui décident de s'y lancer.

La naissance d'un collectif comme AlterNumeris est aussi un signe de changement des mentalités dans le secteur des technologies numériques. Lire des rapports d'experts insistant sur la nécessité de faire valoir le principe de précaution, et de ne pas courir à tout prix dans la direction de la digitalisation à tous les étages, est un indicateur clair que des changements sont en train de s'opérer. Reste à voir si le monde politique y sera réceptif, ou si on continuera à donner des réponses ponctuelles et fragmentaires à ces questions majeures, sans aller au fond du problème.

d. Dans la société civile, de plus en plus de voix contre le tout-au-numérique

Dans la société civile, les voix qui s'élèvent contre le tout-au-numérique pointent le plus souvent les impacts sociaux de la digitalisation, notamment les inégalités engendrées et les problèmes d'accessibilité numérique (ou de fracture numérique). Évoquons par exemple, à la Région de Bruxelles-Capitale, la bataille portée par Lire et Écrire avec environ deux cents autres associations (dont Citoyenneté & Participation) contre l'ordonnance Bruxelles-numérique. Celle-ci, comme l'explique Daniel Flinker (coordinateur du service recherche de Lire et Écrire Bruxelles) dans une analyse de mars 2024, est révélatrice du fait que le numérique est une question politique, et la lutte « *autour d'un symbole (l'ordonnance Bruxelles numérique) et pour des guichets physiques en a été la traduction dans des revendications concrètes* »[88]. Cette bataille et ces problèmes d'inégalités ont également été relayés par des académiques dans une carte blanche publiée en décembre 2023 dans le journal *Le Soir*, où ils appellent à un débat démocratique sur les impacts du numérique : « *À quand le grand débat sur les effets du tout-au-numérique sur nos sociétés* »[89]. La presse alerte de plus en plus sur cette situation. En juin 2024, suite à la publication du dernier baromètre de l'inclusion numérique de la Fondation Roi Baudouin, Philippe Laloux, journaliste au pôle Économie du *Soir*, titre : « *4 Belges sur 10 en état de galère numérique, une urgence démocratique* »[90]. Et la situation est sans aucun doute bien plus grave, étant donné que le Baromètre ne porte que sur les 16-74 ans et que les plus âgés sont ainsi d'emblée déclarés hors course.

Dans la sphère académique, en mars 2024 a eu lieu un colloque sur « L'action publique à l'ère du numérique », organisé par la professeure Elise Degrave, spécialiste en droit du numérique à l'UNamur. Lors de ce colloque, qui a réuni un public très nombreux et varié, une des sections portait sur la question « Numériser sans discriminer ». Y ont été abordées les nombreuses inaccessibilités et inégalités liées à la digitalisation de la société, ainsi que la nécessité de se poser les bonnes questions. Périne Brotcorne, qui travaille depuis plusieurs années au Baromètre de l'inclusion numérique de la Fondation Roi Baudouin, a ainsi indiqué que « *les indicateurs du baromètre* », qui permettent de mesurer l'évolution des États-membres de l'UE en matière d'inclusion numérique, « sous-estiment notamment les effets négatifs d'une connexion généralisée »[91]. La chargée de cours en sociologie à l'UCLouvain a expliqué que depuis cette année, ils ont réussi avec ses collègues, au niveau de Statbel, « *à insérer des questions supplémentaires pour donner une vision un peu plus large que l'accès et l'usage des services essentiels* »[92].

On voit également de plus en plus d'associations proposer des ateliers autour de ces questions : rien que pour Namur, on peut en citer quelques exemples pour 2024 : des ateliers de Déconnexion (comme l'atelier « Désintox numérique » organisé par Canopea en collaboration avec TacTic, Les Amis de la Terre et SympaTic)[93], des ateliers pour sensibiliser à la surveillance généralisée (Les Amis de la Terre)[94], des ateliers interrogeant la digitalisation de la société, dont ses impacts écologiques (au CIEP par exemple, qui a proposé un cycle sur les enjeux de la digitalisation ; ou plus récemment, une matinée de réflexion sur le droit au hors-ligne et la fracture numérique proposée par les Équipes Populaires)[95], etc.

La conscience des nombreux impacts sociétaux liés au numérique grandit, en tout cas dans les champs associatif et académique. Le même constat a récemment été posé en France par la revue Socialter qui, dans un dossier intitulé « Comment échapper à l'emprise du numérique », constate : « *Longtemps inébranlable, le consensus sur les bienfaits de la numérisation du monde semble aujourd'hui se fissurer. Les discours technocritiques sortent peu à peu de la marginalité en France* »[96]. Il est désormais souhaitable que ces questions infusent dans la société dans son ensemble. Le travail d'éducation permanente et de sensibilisation mené par les associations peut être un excellent levier d'action, pour aller, qui sait, jusqu'à une mobilisation citoyenne comme on a pu la voir lors de la bataille contre l'ordonnance « Bruxelles numérique ». L'avenir seul pourra répondre, mais en attendant, on évolue, à petits pas certes, mais un discours qui était complètement inaudible il y a encore quelques années devient de plus en plus accepté et acceptable. Si on veut répondre à l'ampleur des enjeux, il faudra néanmoins aller plus loin et plus vite.

5. La sobriété numérique, mais comment ?

Quelques mesures politiques pour un numérique plus sobre

Pour mettre en place des politiques de sobriété numérique, il faut piloter les usages. Nous souhaitons dans le chapitre suivant pointer quelques mesures qui permettraient de tendre vers davantage de sobriété numérique en Belgique. La liste proposée ci-dessous, dont plusieurs points sont défendus par le Green IT français et/ou ont été mentionnés par Olivier Vergeynst et David Bol dans nos entretiens (voir les notes de bas de page), est loin d'être exhaustive, et les mesures loin d'être détaillées ; notre objectif ici est de donner un aperçu de quelques décisions politiques qui pourraient aller dans le bon sens. Tout en sachant que celles-ci, si elles ne

sont pas partagées au niveau de l'UE – voire au niveau mondial – ont peu de chance d'aboutir à de vrais résultats. Or, la direction numérique de nos États est largement définie aujourd'hui par l'UE, mais aussi par le fonctionnement global du secteur économique du numérique, comme nous l'a bien expliqué David Bol.

Comme autre préalable, notons que de manière générale, ce sont les mesures concernant les entreprises (au moins d'une certaine taille) qui seront les plus significatives, comme nous l'ont confirmé les trois experts que nous avons interrogés. Néanmoins, nos utilisations individuelles des outils numériques ont également des impacts, puisque par le trafic de données qu'elles génèrent (chacun de nos mouvements sur internet étant une source d'argent potentielle pour les courtiers en données personnelles ou data brokers ainsi que pour les géants que sont les GAFAM) et par le stockage nécessaire de celles-ci, elles augmentent les besoins globaux en infrastructures ainsi qu'en énergie. En plus des points mentionnés ci-dessous, la régulation des grandes entreprises qui régissent le net, dont s'est sérieusement emparée l'UE, est donc aussi une manière « *d'agir indirectement sur la pollution numérique* », tout comme « *modifier les comportements des utilisateurs* »[97] (ce dernier point sera développé dans la conclusion). Enfin, nous n'avons pas inclus dans la liste ci-dessous la nécessaire régulation de l'IA, sujet sur lequel nous renvoyons au numéro du magazine Usbek et Rica paru en juillet 2024[98]. On pourrait aussi ajouter à cette liste l'idée de créer un Observatoire du Numérique, comme proposé par Steve Tumson, co-fondateur du collectif AlterNumeris[99], dans un podcast de l'UCLouvain sur « Quelle transition numérique » : un observatoire qui évaluerait « *les impacts des technologies émergentes, pour que le politique fasse des choix éclairés* »[100].

Directive européenne sur les règles communes favorisant la réparation de biens

01. Allonger la durée de vie des produits (ici, numériques)

Allonger la durée de vie des produits, c'est allonger la garantie légale, lutter contre l'obsolescence programmée et logicielle, et agir sur la réparation. Concernant la garantie légale, de nombreuses associations militent pour un allongement de la durée de garantie légale de deux ans à cinq ans. En France, des associations comme les Amis de la Terre et ZeroWaste militent depuis 2015 pour une telle mesure[101], qui n'a pas encore vu le jour. Les pratiques d'obsolescence programmée[102] sont quant à elles pénalisées en France depuis 2015, mais la loi AGEC (loi anti-gaspillage pour une économie circulaire) et la loi REEN (loi pour Réduire l'Empreinte Environnementale du Numérique) ont permis d'étendre cette pénalisation à des pratiques qui jusque-là ne relevaient pas de celle-ci, comme des techniques visant à empêcher la réparation ou à utiliser des techniques logicielles pour réduire la durée de vie des produits[103]. La Belgique pourrait suivre cette voie, tout comme elle pourrait encourager les filières plus durables via des bonus/malus, par exemple en fonction de la taille des écrans, indique Olivier Vergeynst[104]. Le futur indice de durabilité, déjà en vigueur en France mais qui le sera dans les pays de l'UE à partir de 2026, pourrait servir de base à l'instauration de tels bonus/malus.

Sur le plan de la réparation, beaucoup de choses sont en train de changer au niveau européen. Parmi les décisions actées récemment par la proposition de directive européenne sur les règles communes favorisant la réparation de biens[105] : l'allongement de douze mois de la durée de garantie légale si on opte pour la réparation, ou encore l'obligation pour les États-membres de mettre en place au moins une mesure en faveur de la réparation[106]. Néanmoins, comme le souligne l'association RepairTogether, cette directive est malheureusement synonyme d'occasion manquée, car elle est passée à côté de mesures qui auraient pu être bien plus ambitieuses et efficaces, comme « le droit pour le consommateur de faire réparer un produit à moins que cela ne soit factuellement ou légalement impossible » ou encore « l'obligation pour les producteurs de publier toutes les informations relatives à la réparation (telles que les prix de réparation et les prix des pièces détachées) sur leurs sites web », mais une liste exhaustive peut être consultée dans l'excellent article de RepairTogether sur cette directive[107].

En Belgique, un indice de réparabilité pour certains appareils va voir le jour dès 2025, suite à un projet de loi porté par la ministre en charge du développement durable Zakia Khattabi (Ecolo)[108]. C'est l'indice français (depuis 2021, loi AGEC) qui a influencé la loi belge, adoptée à la Chambre le 8 février 2024. Dans la catégorie numérique, seuls les ordinateurs sont concernés par cet indice. Les smartphones et tablettes, contrairement à la France, ne le sont pas car ils recevront à partir de juin 2025 une étiquette énergie qui comportera des informations sur la réparabilité et la durabilité (le règlement a été adopté en même temps que le règlement établissant des exigences en matière d'écoconception[109], et ils entreront tous deux en vigueur en juin 2025)[110]. Notons que si une personne souhaite savoir dès à présent quel est l'indice de réparabilité de l'objet qu'elle s'apprête à acheter, il est possible de faire un détour par le site Ifixit[111], ou encore simplement par un site de vente en ligne français, où l'indice de durabilité est déjà utilisé pour les smartphones.

D'autres mesures pourraient aller plus loin : instaurer des aides à la réparation via un fonds réparation comme celui prévu par la loi AGEC en France, ou encore obliger les producteurs et les vendeurs

à fournir une liste de bonnes pratiques pour entretenir et faire durer l'appareil (nettoyer, ne pas charger trop en applications, utiliser le wifi plutôt que la 4G, etc) ainsi que pour le réparer, etc.

02. Organiser des campagnes d'information sur les impacts environnementaux du numérique et des débats citoyens sur notre société numérisée

Les impacts négatifs du numérique sur l'environnement sont encore largement méconnus du grand public. Les citoyen·ne·s sont plus au fait des enjeux sanitaires et sociaux du numérique que de ses impacts écologiques. C'est pourquoi il faudrait mener des campagnes d'information à grande échelle : des campagnes qui éviteraient le piège dont parle Olivier Vergeynst (celui de lister de « petits gestes » qui ont finalement peu de poids) mais qui au contraire, donneraient vraiment les ordres de grandeur : « *Le vrai enjeu dans les campagnes de sensibilisation, c'est de donner les ordres de grandeur pour que les gens se focalisent sur deux-trois grandes actions : il y en a des milliers, des petites actions, tant mieux si elles sont connues, mais il ne faut pas perdre les gens : il faut vraiment, pour le grand public, se focaliser sur les gros gains* »[112].

Allonger la durée de vie de ses équipements

Quelques exemples : allonger la durée de vie de ses équipements, acheter du reconditionné plutôt que du neuf, faire réparer (si on en a les moyens). Et pour les usages, nous indiquait Olivier Vergeynst, « *c'est principalement la consommation de données dues à la consommation de vidéos puis de photos. Donc on va peut-être essayer par exemple de ne pas regarder des vidéos YouTube ou Netflix en 4K sur un smartphone dans le train, mais si on veut en regarder, mieux vaut diminuer la définition en fonction de la taille de l'écran : ça permet de transmettre moins de données. Plus de données signifie plus d'équipements réseaux, car plus on consomme de données plus on a besoin d'avoir des antennes 4G/5G, etc. Désormais, s'interroger aussi sur nos usages de l'IA… Elle amène des tas d'usages très utiles (domaine médical, économique), mais pour le reste, n'est-on pas capable d'écrire un bout de texte soi-même plutôt que de faire appel à ChatGPT ? Est-il nécessaire de générer automatiquement une vidéo par l'IA, ou autres usages peu utiles mais très énergivores ?* »[113]. Il ne faut pas culpabiliser les citoyen·ne·s, ce sur quoi nos trois interlocuteurs ont bien insisté, mais bien informer sur les impacts, afin que chacun·e puisse poser ses choix le plus consciemment possible.

Par ailleurs, pourquoi ne pas aller plus loin, en organisant des débats citoyens sur la place du numérique dans nos vies ? Cela permettrait de sortir le numérique de la technicité qui le caractérise et qui empêche, comme le souligne le collectif Alter-Numeris, son appropriation citoyenne. D'en refaire un vrai sujet politique. Cela peut se réaliser dans le cadre de l'action associative, mais devrait aussi essaimer en-dehors de ce cadre, avec une impulsion venant du monde politique. L'enseignement pourrait occuper un rôle de première importance dans un tel processus de sensibilisation, comme cela a été décidé en France dans le cadre de la loi REEN. Parmi ses articles, remarquons les articles 1 et 3, qui « *prévoient des modules de formation et de sensibilisation au numérique responsable dans les écoles et les établissements d'enseignement. De plus, les formations d'ingénieur doivent intégrer un module sur l'écoconception des services numériques et à la sobriété numérique. Enfin, l'article 4 prévoit un observatoire des impacts du numérique visant à améliorer la connaissance sur la mesure des impacts directs et indirects du numérique sur l'environnement* »[114].

03. Favoriser le développement de la filière du reconditionnement ainsi que d'une filière de location

La filière du reconditionnement est très peu réglementée actuellement, nous a expliqué Olivier Vergeynst[115]. Si on souhaite donner plus de poids au reconditionné, il faut absolument qu'elle soit davantage structurée. L'impact positif du développement de cette filière, outre l'impact environnemental, a été observé en France pour les territoires et les emplois[116]. Comme la loi AGEC a inspiré la Belgique pour son indice de réparabilité, la loi REEN pourrait encore une fois servir de référence. Celle-ci prévoit notamment que les acheteurs de l'État et des collectivités territoriales doivent « *acquérir certains produits issus du réemploi ou de la réutilisation ou qui comporte des matières recyclées* ». Par exemple l'« *achat de 20 % d'équipements reconditionnés* »[117]. Attention toutefois, alerte Olivier Vergeynst, aux effets rebond : « *Comme il n'y a pas assez d'équipements reconditionnés de qualité sur le marché, il y a un risque important qu'une sorte de filière mixte entre reconditionnement et matériel neuf apparaisse pour que ces acteurs institutionnels puissent acheter du matériel reconditionné ; on se retrouve avec des personnes qui vont reconditionner leur matériel après un an et le racheter parce qu'ainsi, ils respectent la loi, alors qu'en réalité on n'a rien gagné d'un point de vue environnemental* »[118]. C'est pourquoi le directeur de l'Institut Belge du Numérique Responsable insiste d'abord sur les aides permettant à une filière solide de reconditionnement de se développer, pour ensuite greffer sur celle-ci des obligations d'achats de reconditionné.

Une autre mesure ambitieuse pourrait résider dans des aides publiques à des structures qui proposeraient de la location de matériel (à l'instar de la coopérative Commown en France)[119].

04. Interdire la vente couplée d'équipements neufs avec de nouveaux abonnements[120]

Pour envoyer un signal fort, une autre mesure politique pourrait résider dans l'interdiction de certaines ventes couplées, en l'occurrence toutes les offres permettant d'acquérir un smartphone neuf, souvent à très bas prix – voire gratuitement ! – moyennant la souscription à un nouvel abonnement. Comme le souligne l'association Les Amis de la Terre France, « *conditionner le renouvellement d'un abonnement – en général tous les deux ans – à l'offre d'un nouveau smartphone est une machine à remplacer les produits prématurément* »[121]. Cela devrait également s'appliquer à tout équipement numérique dont l'achat serait encouragé par la souscription à un abonnement. Pour une telle mesure, c'est d'abord sur la législation européenne qu'il faudrait agir, pour que cette pratique soit répertoriée comme déloyale. En effet, en Belgique, les offres couplées ont été interdites jusqu'en 2009. À cette date, l'interdiction a été levée suite à une condamnation de la Belgique par la Cour européenne de justice. La directive européenne du 11 mai 2005[122] avait effectivement établi un recensement des pratiques commerciales considérées comme déloyales dans l'UE, et comme les offres couplées n'étaient pas considérées comme telles, la Belgique ne pouvait appliquer une législation plus restrictive[123]. En attendant, il serait possible, par exemple instaurer l'obligation pour les points de vente d'informer sur les offres couplées de téléphones reconditionnés.

L'idée de certificats de sobriété numérique

05. Pour les entreprises, mieux réglementer la mesure de l'empreinte carbone et imposer des mesures contraignantes[124]

Pour Olivier Vergeynst, « *la difficulté est de trouver les mesures qui ont un vrai impact environnemental. Une des façons d'y arriver serait de mieux réglementer la mesure de l'empreinte carbone du numérique en scope 1, 2 et 3*[125]*, y compris l'utilisation par les clients. Cela devrait être fait au niveau européen, car c'est très mal mesuré aujourd'hui. La première étape serait donc de se mettre d'accord sur une manière de mesurer qui ne soit pas trop influencée par les lobbies du numérique. Et ensuite, comme pour tout ce qui concerne l'empreinte carbone, de mettre un prix suffisant pour que les entreprises aient un intérêt à la réduire, tout en gardant à l'esprit que l'empreinte environnementale est bien plus que l'unique empreinte carbone…* »[126].

On pourrait donc imaginer des taxes mais aussi des incitants financiers. La taxation permettrait d'assurer un suivi de ce que font les entreprises en termes d'intelligence artificielle, par exemple : l'utilisation de l'IA est-elle nécessaire ? S'intègre-t-elle dans une logique IT for human ou est-elle « gratuite » ? Tout ce qui est extrêmement gourmand en données ne devrait être utilisé que de façon mesurée. Certains chercheurs avancent l'idée de certificats de sobriété numérique, à l'instar des certificats d'efficacité énergétique[127].

Quant aux incitants : aujourd'hui, les structures (publiques, privées) peuvent décider d'être accompagnées par l'Institut Belge du Numérique Responsable pour tendre vers un numérique plus durable, mais pour l'instant, aucun incitant financier n'existe. Une première mesure pourrait résider dans des aides financières de taille pour les structures qui prennent cette direction. Les appels d'offres, également, pourraient être conditionnés à ce critère du numérique durable : « *pour l'instant, en Région de Bruxelles-capitale, ça peut permettre de départager deux dossiers qui seraient équivalents en qualité, mais ça pourrait aller beaucoup plus loin* »[128].

Et bien sûr, continuer à réguler les géants du net et le business des données personnelles, qui sont responsables d'une part non négligeable de la pollution numérique.

06. Instaurer un service internet "post-croissance" au niveau des opérateurs télécom[129]

Une idée qui pourrait fonctionner au niveau national, selon le professeur David Bol, que nous avons interrogé dans le cadre de ce travail, serait d'agir au niveau des opérateurs télécom, qui sont des acteurs souffrant de peu de concurrence au niveau international et pour lesquels les pays ont la capacité de légiférer. « *En se disant qu'on a déjà des capacités de service extrêmement importantes à l'heure actuelle, on pourrait décider de les maintenir sans nécessairement vouloir les améliorer avec de nouveaux usages d'internet dans les années à venir* ». Cela nécessiterait toutefois « *d'arbitrer sur les usages en amont* », afin de ne pas saturer le réseau. « *Définir quels usages seraient prioritaires, quels usages seraient acceptables s'il y a de la bande passante, et quels usages on bannirait, nécessite bien sûr des choix politiques* ». En effet, un principe important dans le numérique tient « *dans la neutralité d'internet : les opérateurs ne peuvent pas faire cet arbitrage. Cette neutralité a une raison d'être : celle d'éviter le totalitarisme ou la mainmise d'opérateurs privés ou d'États sur la sélection des contenus. Il faudrait donc une recherche pour définir quels seraient les bons moyens légaux d'un côté, et d'un point de vue sociologique et éthique de l'autre, pour établir cette priorisation. Ces choix pourraient être opérés de*

manière démocratique par les instances politiques ou par la consultation citoyenne »[130].

07. Interdire ou, a minima, limiter la publicité pour le numérique (offres de data illimitées, smartphones à douze euros, etc.) dans les espaces publics

Enfin, une mesure qui serait urgente et indispensable – et qui ne concerne pas que le numérique : l'élimination ou, a minima, la limitation de la publicité privée dans les espaces publics, comme cela a été décidé pour Grenoble, par exemple, depuis dix ans déjà[131]. Si une interdiction totale semble utopique pour le moment en Belgique, il pourrait être décidé qu'à l'instar d'autres produits problématiques pour la santé, tout ce qui concerne le numérique soit également régulé, voire interdit, de publicité… Mais nous en sommes loin. En observant les écrans publicitaires de certains endroits de la ville de Namur récemment, nous avons eu l'impression que nombre de publicités concernent de la malbouffe, ou des équipements ou abonnements numériques[132].

Par ailleurs, pour aller dans le sens de l'exemplarité en termes de sobriété, il faudrait également que les villes envisagent une suppression des écrans publicitaires dans les lieux publics[133].

08. Mais aussi, un nécessaire changement dans le secteur économique de la production d'équipements numériques[134]

Pour David Bol, il y a toutefois un point crucial qui empêche le secteur du numérique d'adresser l'enjeu de la réduction de l'empreinte environnementale : il s'agit du fait que « *ce secteur est structuré autour d'une série de lois empiriques sur lesquelles les entreprises s'alignent pour faire fonctionner leur business modèle. La loi la plus structurante parmi celles-ci est la loi de Moore* ». Il s'agit d'une « *loi économique, qui nous dit qu'en mettant plus de transistors par puce électronique, tous les deux ans environ, on est capable de génération en génération d'avoir de plus en plus de fonctionnalités pour un coût marginal de la puce assez stable. Ça crée donc du business, puisque tous les deux ans il y a des fonctionnalités en plus, permettant de vendre un nouveau dispositif* ». Tout le secteur du numérique est donc basé sur cette loi, sur le fait que les performances évoluent de manière exponentielle avec le temps. Le problème, nous explique David Bol, est que « *parvenir à miniaturiser les transistors devient de plus en plus difficile avec le temps car on se rapproche d'une limite physique qui est celle de l'atome de silicium, la matière constituant la tranche de la puce électronique* ». Donc, plus c'est compliqué, plus ça demande d'argent et de moyens. Pour réussir à générer un retour sur investissement, un double effet-rebond se crée par conséquent : premièrement, ces entreprises vont vendre plus, donc produire plus ; deuxièmement, pour produire, les besoins en énergie et en matériaux croissent. David Bol considère que si l'industrie ne prend pas conscience du fait qu'il faut sortir de ce business modèle pour réduire les impacts environnementaux, le levier de l'économie circulaire, « *qui a pourtant beaucoup de sens, ne sera pas un levier avec des impacts réels* » : « *en effet, donner une deuxième vie à un appareil ou étendre sa durée de vie ne fonctionne que si on réduit les volumes de production en amont. Si on continue à faire grandir les volumes de production, on se retrouve simplement avec plus d'équipements en usage en permanence… Si on fait durer les téléphones plus longtemps, on va fabriquer des objets connectés pour écouler les stocks de la production électronique* ». C'est pourquoi nous souhaitions terminer ce chapitre sur cet élément qui nous semble fondamental : ce n'est donc pas seulement au niveau de l'UE que de nombreux changements vont devoir s'opérer, mais également au niveau mondial. D'autant plus qu'aujourd'hui, « *la question de la souveraineté technologique est de plus en plus présente, et que plusieurs continents dont l'Europe ont décidé de se doter de chaînes d'approvisionnement locales : mais une localisation de la production sur le continent pourrait être une bonne nouvelle si elle se substituait partiellement à celle localisée en Asie. Or, on observe plutôt une production supplémentaire. On est donc face à une montagne en termes d'infléchissement des tendances* »[135].

La limitation de la publicité privée dans les espaces publics

Ces éléments, que nous ne pouvions taire car ils sont à la base de tout le fonctionnement du secteur numérique, ne doivent toutefois pas nous empêcher de continuer à réfléchir et à agir au niveau local, sur les éléments tangibles sur lesquels nous avons prise, afin de nous approprier ou de nous ré-approprier la question de la place du numérique dans nos vies. Pour ce faire, nous proposons, pour conclure cette étude, une réflexion sur des « pistes individuelles et collectives pour sortir du techno-capitalisme », pensées comme autant de petites graines d'inspiration pour nos lecteurs et lectrices, en espérant que celles-ci puissent trouver résonance en eux, en elles.

Conclusion : des pistes individuelles et collectives pour sortir du techno-capitalisme

Nous disions en introduction que la sobriété numérique était plus un horizon collectif qu'individuel. Mais la sobriété numérique individuelle est sans doute un excellent point de départ pour une conscientisation plus large de la société, puisqu'elle est, on l'a vu, avant tout une prise de conscience : à titre individuel, réaliser qu'on fait un usage trop fréquent des outils numériques, quels qu'ils soient, est donc déjà un grand pas. La mise en pratique en est un autre, plus difficile à mettre en œuvre, car elle implique d'aller à contre-courant. C'est donc en s'entourant que l'on peut avancer plus vite dans une démarche de « désintoxication numérique », en parlant de ces questions, en partageant une éventuelle démarche de sobriété personnelle (ou une simple interrogation), et en laissant infuser. Frédéric Bordage mentionne aussi la nécessité de « s'entourer de connaissances fiables et d'acteurs à la fois sincères et experts », afin d'éviter les actes vendus par le greenwashing, qui sont inutiles ou de faible impact[136]. Ainsi, une connaissance des actions qui peuvent vraiment faire la différence est indispensable. Et ces actions ne sont finalement pas pratico-pratiques comme on pourrait le croire (effacer ses mails, aller sur un navigateur vert ou ce genre de choses), mais sont plutôt de l'ordre de la réflexion et d'un questionnement global sur les besoins. Pour le smartphone, Hélène Petit, autrice d'un livre sur la sobriété numérique sorti en 2023, identifie trois astuces pour limiter les usages excessifs :

- Supprimer les usages non indispensables ;
- Limiter au maximum les notifications ;
- « *Reprendre le contrôle sur notre téléphone pour qu'il soit un outil à notre service* », et pas pour que nous soyons en permanence connecté à lui, dans un besoin irrépressible d'instantanéité[137].

Même réflexion pour Olivier Vergeynst : « *L'essentiel, c'est questionner les besoins* »[138]. Ce qui nous ramène à la démarche low-tech telle que théorisée par Philippe Bihouix, dont nous avons déjà parlé dans une récente analyse[139] : interroger la durabilité, interroger l'accessibilité, interroger les besoins.

Au niveau individuel, mais aussi et surtout, au niveau collectif et donc, dans l'action publique. Dans la conclusion de sa communication lors du colloque « L'action publique à l'ère du numérique » en mars 2023, Périne Brotcorne, déjà citée plus haut, a conclu sur l'excellente porte d'entrée que propose Philippe Bihouix, dont les questionnements devraient être « *essentiels quand on développe des services publics pour l'intérêt général* » : « *Quelle est la plus-value de chaque technologie, quelle est son utilité (faire preuve de techno-discernement) ? Quelle est l'accessibilité, donc l'appropriation possible de cette technologie ? Et enfin, les technologies numériques en voie de conception sont-elles en adéquation avec les limites des ressources planétaires ?* »[140].

Ces questions sont une porte d'entrée, mais on voit aussi les limites que cela comporte. On a beau savoir, on continue sur notre lancée. Quelles autres portes d'entrée alors ? Nos lectures, surtout celle d'Alain Damasio, nous soufflent une réponse en deux temps :

- L'information et l'éducation
- La recréation d'espaces de lien, qui manquent cruellement à notre société.

L'information et l'éducation ont un rôle de premier plan à jouer dans les réflexions sur nos usages du numérique et sur les avenirs souhaitables. Pour que la sobriété numérique puisse devenir un horizon positif et non plus synonyme uniquement de privation, il importe non seulement d'informer, mais d'éduquer au numérique (d'autant plus depuis l'apparition de l'IA), dans un vrai programme qui irait bien plus loin que de « simplement éduquer au numérique ». En sachant qu'une grande difficulté, pour les formateurs/enseignants eux-mêmes, est de réussir à se tenir à jour, face aux multiples nouveautés qui apparaissent chaque jour dans le domaine. Il y a encore deux ans, ChatGPT n'existait pas : il bouleverse déjà aujourd'hui le secteur de l'enseignement…

Sur la nécessité de développer une éducation complète au numérique, je laisse la parole à Alain Damasio qui, dans son livre Vallée du Silicium[141], offre un passage inspirant :

> Alors il est peut-être temps d'éduquer : éduquer à l'ancienne, éduquer inversé, s'auto-éduquer et s'entre-éduquer, des parents aux enfants et des enfants aux parents, à la maison, en classes bleues, dans des assoces, dans des tiers-lieux, par l'éducation populaire ou experte, en ville comme à la campagne, à l'aide des pirates et des hacktivistes. Et même éduquer, rêvons debout, sous l'égide de l'Éducation nationale, où la techno doit passer de matière-poubelle décérébrée à un statut aussi crucial que le français et les maths pour émanciper nos collégiens et nos lycéens par la connaissance et la pratique lucide des réseaux. Éduquer d'accord, vous me direz, mais à quoi ? À ce qui fait nos routines et nos quotidiens d'utilisateurs, déjà. À la manipulation de notre attention, ensuite. À la prise de distance. Et interroger. Pour ouvrir les crânes, pour sortir des tunnels stimuli-réactions. Interroger tout ce que le numérique transforme en nous, sans cesse, et

> tout ce que ça traverse. Interroger la psychologie que ça mobilise, les rapports sociaux que ça forme, les enjeux philosophiques que ça soulève, et la politique qui en découle. Interroger ce que peut encore l'État, ce que peuvent encore défendre ou réguler le droit et les lois. […]
> Questionner l'idéal de fluidité et de facilité, l'ergonomie molle ;
> Discuter l'impact des technos sur la planète, sur notre santé, sur nos cancers, sur nos déchets, sur la misère ;
> Décomposer les rythmes machiniques, montrer comment la techno désynchronise la vie sociale, la stresse ou la bloque, l'accélère ou la sature ;
> Interroger l'idéal de continuité de service et de performance ;
> Apprendre la déconnexion, la coupure […] ;
> Former aux low-techs, privilégier les ateliers où on fait soi-même.

Sur le recréation d'espaces de lien, revenons encore une fois à Damasio : en 2021, l'écrivain, entouré d'un collectif, a fondé L'École des vivants, un lieu qui est « *une zone d'expérimentations. Élevage, maraîchage, stages de théâtre, de clown, d'écriture ou de "polytique", résidence d'artistes et d'écrivains […] Un lieu pour se transformer, individuellement et collectivement, et sortir du techno-cocon* »[142]. Damasio explique : « *Travailler sur le lien, retisser des liens humains suffisamment riches, denses, […] car le néo-libéralisme a toujours vendu le contraire […] : la liberté ne peut être conçue que d'une seule manière et c'est la liberté individuelle […] Il faut donc du lien humain, intense, incarné, retrouvé, avec cette dimension corporelle qui aujourd'hui est complètement dématérialisée* »[143]. Dans le même esprit, Frédéric Bordage en appelle « à créer des oasis de sobriété numérique ».

Revenir au lien au vivant est également fondamental pour l'écrivain, qui constate : « *On vit toujours avec un dualisme nature-culture. […] Le lien est complètement coupé. Si tous les liens sont retissés, re-tramés, tu retrouves de la puissance et c'est plus fort que le techno-capitalisme* »[144]. C'est donc un nouveau récit collectif plus fort que le scénario techno-capitaliste qu'il nous faut construire. Si la réponse ne vient pas du monde politique, gageons qu'elle puisse venir de la société civile, qui tel le colibri, pourrait faire sa part, et remonter à nos dirigeant·e·s que le monde dans lequel nous souhaitons vivre n'est pas celui qu'on nous offre, et qu'un avenir dans lequel le numérique serait pensé, réfléchi, interrogé collectivement à la hauteur des enjeux qu'il soulève, est possible. Qu'ensemble, nous puissions faire en sorte que le numérique continue à servir l'humain, sans que l'humain y soit assujetti, et en respectant les limites de notre planète. Que nous puissions dessiner un avenir où tout est possible, où des liens se tissent autour des technologies et où l'on en débat ; où l'on fait sortir le numérique de l'emprise de multinationales privées avides d'argent ; un avenir, surtout, qui soit plus désirable que le scénario techno-capitaliste actuel. Un avenir où les imaginaires se libèrent pour construire un meilleur vivre-ensemble. Voici, à notre avis, un programme enthousiasmant à prendre à bras-le-corps, individuellement, collectivement, démocratiquement, philosophiquement, poétiquement, pour relever un des défis majeurs de ces prochaines décennies.

[1] On pourrait dire que l'enjeu est similaire à celui de tous les actes écologiques : rouler à vélo plutôt qu'en voiture est un acte important – il ne faut pas se décourager – mais est peu significatif si à côté de cela, le kérosène des avions reste non taxé à hauteur des émissions engendrées ; appeler de nos vœux une agriculture durable et une alimentation saine reste peine perdue si la publicité pour la malbouffe n'est pas interdite (voir sur ce dernier sujet l'édition de mars 2024 de la revue Tchak !, intitulée « Le colibri, ça suffit ! »), etc. Les exemples sont légion.

[2] Autissier I., Préface de Bordage, Frédéric, Sobriété numérique. Les clés pour agir, Paris, Libella, 2019, p. 11.

[3] Par exemple en terme de recherche et d'avancées médicales, de démocratisation et de partage de l'information, mais aussi d'aide pour relever certains défis du XXIe siècle, etc.

[4] Damasio A., Vallée du Silicium, Paris, Seuil/Albertine, 2024, p. 191.

[5] *Ibid.*

[6] Nous remercions également David Bol et Olivier Vergeynst pour leur relecture.

[7] Sur cette polarisation, voir Alternumeris (auteurs Tumson S., Raone J., Coma M., et plusieurs contributeurs), Faire cohabiter numérique et environnement ? La contribution de trois regards croisés, février 2024, p. 2, [en ligne :] https://www.alternumeris.org/faire-cohabiter-numerique-et-environnement/, consulté le 14 mai 2024.

[8] Hamant O., De l'incohérence. Philosophie politique de la robustesse, Paris, Odile Jacob, 2024, p. 167.

[9] *Ibid.*, p. 169.

[10] Bordage F., Tendre vers la sobriété numérique. Je passe à l'acte, Paris, Actes Sud, 2001, p. 6.

[11] Alternumeris, Faire cohabiter […], p. 3. Il s'agit d'un élément de convergence des très nombreux rapports de qualité et de méthodologie diverses pointés par le collectif.

[12] Impact environnemental du numérique en 2030 et 2050. L'ADEME et l'ARCEP publient une évaluation prospective, Communiqué de presse, 6 mars 2023, [en ligne :] https://presse.ademe.fr/2023/03/impact-environnemental-du-numerique-en-2030-et-2050-lademe-et-larcep-publient-une-evaluation-prospective.html, consulté le 14 mai 2024.

[13] Ademe, Transition(s) 2050. Choisir maintenant, agir pour le climat. Nouvelle édition 2024, téléchargeable à l'adresse https://librairie.ademe.fr/recherche-et-innovation/5072-prospective-transitions-2050-rapport.html, p. 58, consulté le 4 juin 2024.

[14] Voir à ce sujet Hadjadji N., « L'insoutenable coût écologique du boom de l'IA », Reporterre, 4 juillet 2024, [en ligne :] https://reporterre.net/L-insoutenable-cout-ecologique-du-boom-de-l-IA, consulté le 30 août 2024.

[15] Voir à ce sujet Fronteddu B., « Pacte vert européen. La matérialité d'une double transition », Citoyenneté & Participation, analyse n°474, juillet 2023, p. 9, [en ligne :] https://www.cpcp.be/publications/pacte-vert-europeen-double-transition/, article repris dans ce cahier.

[16] Alternumeris, *op. cit.*, p. 3.

[17] Fronteddu B., *op. cit.*, p. 5, citant Carolan J., « Digital Devices Took Over Our Lives in 2020 : Here's How to Stay Secure », Forbes.com, 15 avril 2021, [en ligne :] https://www.forbes.com/councils/forbes-techcouncil/2021/04/15/digital-devices-took-over-our-lives-in-2020-heres-how-to-stay-secure/, consulté le 4 juin 2024.

[18] Petit H., La sobriété numérique. Comment rester connecté en conscience, Paris, Ulmer, 2023, p. 25.

[19] Gemenne F., Rankovic A., Atelier de cartographie de Sciences Po, Atlas de l'anthropocène. Deuxième édition actualisée et augmentée, Paris, Presses de Sciences Po, 2021, p. 119.

[20] Bordage, *op. cit.*, p. 9.

[21] Entretien avec Olivier Vergeynst, directeur de l'Institut Belge du Numérique Responsable, 29 mai 2024.

[22] Bordage, *op. cit.*, p. 9.

[23] Le collectif AlterNumeris a pour objectif de permettre au citoyen de s'approprier des réflexions souvent réservées aux experts : « donner aux citoyens les clés pour comprendre, les arguments pour débattre et les moyens pour se positionner ». Leur travail est voué à « politiser la société numérique » c'est-à-dire à « ouvrir le champ de ses possibles, la condition pour que ses orientations, ses finalités et ses usages soient délibérées par le plus grand nombre. Alors seulement, le numérique peut devenir porteur de sens et d'émancipation » (voir le site internet du collectif : https://www.alternumeris.org/le-collectif-alter-numeris/, consulté le 3 juin 2024).

[24] Alternumeris, *op. cit.*, p. 3.

[25] *Ibid.*, p. 25.

[26] *Ibid.*

[27] bid., p. 3, p. 37.

[28] Voir à ce sujet l'article précité de Boris Fronteddu dans ce volume, « Pacte vert européen », ainsi que Leterme, Cédric, « Transitions jumelles : Pourquoi les agendas vert et numérique européens s'opposent au lieu de se renforcer », Gresea, 3 juin 2024, [en ligne :] https://gresea.be/Transitions-jumelles-Pourquoi-les-agendas-vert-et-numerique-europeens-s, consulté le 29 août 2024.

[29] Nous reprenons une expression du rapport Sobriété numérique du Shift Project ((laboratoire d'idées français visant à proposer des solutions pour décarboner l'économie) : Déployer la sobriété numérique. Rapport complet, octobre 2020, téléchargeable à l'adresse : https://theshiftproject.org/article/deployer-la-sobriete-numerique-rapport-shift/, p. 2, consulté le 3 septembre 2024.

[30] *Ibid.*

[31] Trésor de la Langue française Informatisé : http://stella.atilf.fr/Dendien/scripts/tlfiv5/advanced.exe?8;s=1654494315, consulté le 30 mai 2024.

[32] Entretien avec Olivier Vergeynst, 29 mai 2024.

[33] Frédéric Bordage, Les clés […], *op. cit.*, p. 155.

[34] Entretien avec Olivier Vergeynst, 29 mai 2024.

[35] *Ibid.*

[36] Les études de référence manquent en Belgique ; elles sont plutôt françaises et une étude a aussi été réalisée au niveau européen à la demande du groupe des Verts, mais on peut extrapoler les chiffres français pour la Belgique sans trop de risques, nous a expliqué Olivier Vergeynst, sauf pour l'impact des usages en matière d'électricité, le mix énergétique français étant très décarboné.

[37] Étude Ademe-Arcep sur l'empreinte environnementale du numérique en 2020, 2030 et 2050, Dossier de presse, téléchargeable à l'adresse https://www.arcep.fr/la-regulation/grands-dossiers-thematiques-transverses/lempreinte-environnementale-du-numerique/etude-ademe-arcep-empreinte-environnemental-numerique-2020-2030-2050.html, p. 3, consulté le 11 juin 2024.

[38] Voir à ce sujet l'étude d'Alternumeris, Faire cohabiter […], pp. 28-34.

[39] Alternumeris, Faire cohabiter […], *op. cit.*, p. 5.

[40] *Ibid.*, p. 3, p. 14.

[41] Sur les investissements colossaux de Musk dans la conquête de l'espace, voir l'excellente étude de Philippe Courteille « Les dangers démocratique du numérique », dans ce Cahier.

[42] Ademe, Impact environnemental du numérique en 2030 et 2050, *op. cit.*, consulté le 21 juin 2024.

[43] Bordage, Tendre vers la sobriété numérique, *op. cit.*, p. 19.

[44] Entretien avec Olivier Vergeynst, 29 mai 2024.

[45] *Ibid.*

[46] Entretien avec Louise Marée, 3 juillet 2024.

[47] The Shiftproject, Déployer la sobriété numérique. Rapport complet, octobre 2020, téléchargeable à l'adresse : https://theshiftproject.org/article/deployer-la-sobriete-numerique-rapport-shift/, p. 2, consulté le 4 juin 2024.

[48] Nous renvoyons sur ce point à trois textes de ce Cahier : l'étude précitée de Philippe Courteille sur Numérique et Démocratie, l'analyse de Roxane Lejeune sur l'impact des écrans sur la santé et celle de Boris Fronteddu sur le business des données personnelles.

[49] Damasio A., interviewé par Reporterre à l'occasion de la sortie de son livre Vallée du Silicium, [en ligne :] https://reporterre.net/Alain-Damasio-Il-faut-battre-le-capitalisme-sur-le-terrain-du-desir, consulté le 28 juin 2024.

[50] Ademe, Les futurs en transition. Les scénarios, [en ligne :] https://www.ademe.fr/les-futurs-en-transition/les-scenarios/, consulté le 4 juin 2024. Sur ce travail, l'ADEME souligne : « L'ADEME a souhaité soumettre au débat quatre chemins "types" cohérents qui présentent de manière volontairement contrastée des options économiques, techniques et de société pour atteindre la neutralité carbone en 2050. Imaginés pour la France métropolitaine, ils reposent sur les mêmes données macroéconomiques, démographiques et d'évolution climatique (+2,1 °C en 2100). Cependant, ils empruntent des voies distinctes et correspondent à des choix de société différents. Ce travail a été conduit de 2019 à 2021. Pour autant, la crise Covid-19 et le conflit en Ukraine ne remettent en cause ni les hypothèses ni les conclusions du travail présenté ici. Au contraire, ils les renforcent en montrant l'intérêt de la sobriété et de s'affranchir des énergies fossiles ».

[51] Ademe, Transition(s) 2050, *op. cit.*, p. 58, consulté le 4 juin 2024

[52] *Ibid.*

[53] Alternumeris, Faire cohabiter […], *op. cit.*, p. 15.

[54] *Ibid.*

[55] *Ibid.*

[56] Ademe, Transition(s) 2050, *op. cit.*, pp. 36-37.

[57] Le lien est établi dans le rapport d'AlterNumeris sur Numérique et environnement précité, p. 15 : « Dans un précédent rapport, AlterNumeris approchait la question du développement de la 5G au départ des imaginaires politiques. Notre rapport au numérique en général, et aux politiques du numérique en particulier, est nourri de manières de penser l'innovation et la place des technologies. Elles reposent sur des visions du monde, des représentations de la vie sociale et du sens de nos actions qui tapissent nos liens à la technique. Dans une démarche comparable quoique prospective, l'Agence De l'Environnement et de la Maîtrise de l'Energie (ADEME), organisme chargé d'accompagner l'État français dans la transition écologique et énergétique, envisage 4 scénarios d'articulation des transitions à l'horizon 2050 ».

[58] Alternumeris, La 5G, au-delà du « pour ou contre, p. 30, [en ligne :] https://www.alternumeris.org/la-5g-au-dela-du-pour-ou-contre/, consulté le 6 juin 2024.

[59] Alternumeris, Faire cohabiter […], *op. cit.*, pp. 19-20.

[60] Voir à ce sujet Fronteddu B., Pacte vert européen […], *op. cit.*

[61] Nous reprenons ici une réflexion de Périne Brotcorne au colloque « L'action publique à l'ère du numérique », UNamur, 15 mars 2024.

[62] Entretien avec Olivier Vergeynst, 29 mai 2024.

[63] *Ibid.*

[64] Société dont la mission est d'aider les organisations à réduire leur impact sur le climat en vue de la neutralité carbone pour 2050 (voir https://climact.com/fr/about/, consulté le 17 juin 2024).

[65] Entretien avec Olivier Vergeynst, 29 mai 2024.

[66] Climact, Quel est l'impact du secteur numérique sur la consommation d'électricité et les objectifs climatiques de la Wallonie ?, 22 janvier 2021, [en ligne :] https://climact.com/fr/quel-est-limpact-du-secteur-numerique-sur-la-consommation-delectricite-et-les-objectifs-climatiques-de-la-wallonie/, consulté le 17 juin 2024.

[67] Agoria, Digital4Climate, téléchargeable ici : https://www.agoria.be/fr/etude-digital4climate.

[68] Entretien avec Olivier Vergeynst, 29 mai 2024.

[69] Voir Samain M., « Le numérique pourrait réduire les émissions belges de C02 de 10%, selon Agoria », L'Écho, 3 mai 2022, [en ligne :], https://www.lecho.be/entreprises/technologie/le-numerique-pourrait-reduire-les-emissions-belges-de-co2-de-10-selon-agoria/10385339.html, consulté le 24 mai 2024.

[70] Alternumeris, Faire cohabiter […], *op. cit.*, pp. 29-34.

[71] Agence du numérique, Étude Numérique et environnement, 3 mars 2022, [en ligne :] https://www.digitalwallonia.be/fr/publications/dossier-numerique-environnement-1/, consulté le 12 juin..

[72] Deliège F., Partie 1, « Principaux constats », dans *Ibid.*

[73] https://www.digitalwallonia.be/fr/publications/numerique-environnement-regards-croises/, consulté le 21 juin 2024.

[74] Alternumeris, Faire cohabiter […], *op. cit.*, p. 5 et p. 37.

[75] L'agence du numérique est un centre d'expertise et le conseiller privilégié du Gouvernement wallon et de la Wallonie en termes de transformation numérique du territoire. Voir https://www.adn.be/fr/, consulté le 4 juin 2024.

[76] Cette stratégie de numérisation nous semble en l'état actuel se situer dans le scénario 4 de l'ADEME, c'est-à-dire celui du techno-capitalisme, impression confirmée par le rapport d'AlterNumeris où le détail de la stratégie wallonne apparaît dans le scénario techno-capitaliste : Alternumeris, Faire cohabiter, *op. cit.*, p. 19.

[77] Entretien avec Louise Marée, 3 juillet 2024.

[78] DigitalWallonia4Circular, Évaluation du potentiel des technologies numériques pour l'économie circulaire en Wallonie, Agence du Numérique, expert : Louise Marée ; rédaction : Garance Wauthier, [en ligne :], téléchargeable à l'adresse https://www.digitalwallonia.be/fr/publications/numerique-circularite-potentiel/, consulté le 30 août 2024.

[79] *Ibid.*, p. 7.

[80] bid, p. 8.

[81] Entretien avec Louise Marée, 3 juillet 2024.

[82] Entretien avec David Bol, 1er juillet 2024.

[83] Voir « DPR 2024-2029. La transformation numérique au service de la Wallonie, de ses habitants et de ses entreprises », article publié sur le site Digital Wallonia, 14 août 2024, https://www.digitalwallonia.be/fr/publications/strategie-digital-wallonia-dpr-2024-2029/, consulté le 2 septembre 2024.

[84] Entretien avec Olivier Vergeynst, 29 mai 2024.

[85] *Ibid.*

[86] Même si ce n'est pas une initiative de nos pouvoirs publics, mais bien une initiative de l'ordre de l'associatif, puisque l'Institut est une ASBL.

[87] Les quatre volets sont :

- comment on réduit l'impact environnemental du numérique (Green IT), 75%-80% du travail de l'Institut.
- comment est-ce qu'on utilise le numérique pour diminuer notre empreinte dans d'autres domaines (IT for green).
- comment est-ce qu'on crée des applications et services qui génèrent moins de problèmes d'exclusion, d'inaccessibilité, comment on gère l'éthique dans l'IA par exemple (IT for Human).
- comment est-ce qu'on crée des services au service de la société plutôt que des GAFAM (Human for It).

[88] Flinker D., « De quoi la campagne contre l'ordonnance Bruxelles numérique est-elle le révélateur ? », Lire et Écrire, mars 2024, [en ligne :] https://lire-et-ecrire.be/De-quoi-la-campagne-contre-l-ordonnance-Bruxelles-numerique-est-elle-le, consultée le 17 juin 2024.

[89] Brotcorne P., *et al.*, « À quand le grand débat sur les effets du tout-numérique sur nos sociétés », carte blanche, Le Soir, 5 décembre 2023, [en ligne :] https://www.lesoir.be/553415/article/2023-12-05/quand-le-grand-debat-sur-les-effets-du-tout-numerique-sur-nos-societes, consulté le 17 juin 2024.

[90] Laloux P., « 4 Belges sur 10 en état de galère démocratie, une urgence démocratique », Le Soir, 14 juin 2024, [en ligne :] https://www.lesoir.be/595027/article/2024-06-14/4-belges-sur-10-en-etat-de-galere-numerique-une-urgence-democratique, consulté le 17 juin 2024.

[91] Communication de Périne Brotcorne au colloque « L'action publique à l'ère du numérique », UNamur, 15 mars 2024, notes personnelles, validées par l'oratrice.

[92] *Ibid.*

[93] Voir : https://www.tacticasbl.be/agenda/atelier-desintox-numerique-retrouvons-notre-liberte-dusage-ou-de-non-usage-des-outils-numeriques-2/.

[94] Voir : https://www.amisdelaterre.be/events/event/surveillance-generalisee-1er-atelier/.

[95] Voir : https://www.ciep.be/index.php/558-numerisation-de-la-societe-quels-enjeux-2024 et https://www.equipespopulaires.be/events/numerique-un-peu-beaucoup-a-la-folie-pas-du-tout/.

[96] Gautier E., « Attention : fragile », Socialter n°64, Peut-on échapper à l'emprise numérique, juin-juillet 2024, pp. 18-21, p. 20.

[97] Voir à ce sujet Nicolaï, Jean-Philippe et Peragin, Lise, « Les certificats de sobriété numérique comme instrument de régulation de la pollution numérique », Revue de l'OFCE, p. 234, [en ligne :] https://shs.cairn.info/revue-de-l-ofce-2022-1-page-229?lang=fr, consulté le 29 août 2024, p. 234.

[98] « Intelligence Artificielle. 10 propositions pour reprendre le contrôle », Usbek et Rica, juillet 2024.

[99] Steve Tumson est ingénieur Civil Mécatronicien de l'UCL, expert en robotique, aujourd'hui consultant, conférencier et professeur (voir https://www.alternumeris.org/le-collectif-alter-numeris/).

[100] Podcast « Quelle transition numérique », https://www.podcastics.com/podcast/episode/quelle-transition-pour-le-numerique-309021/, consulté le 5 novembre 2024. La création d'un observatoire du numérique fait partie des exemples de leviers cités pour le programme social-démocrate dans la partie du rapport d'AlterNumeris consacrée aux programmes d'action publique (voir AlterNumeris, Faire cohabiter […], *op. cit.*, p. 20.

[101] « Augmenter la durée de la garantie légale de conformité », HOP, 19 août 2015, [en ligne :] https://www.halteobsolescence.org/augmenter-la-duree-de-la-garantie-legale-de-conformite/, consulté le 6 juin 2024.

[102] Sur l'obsolescence programmée, voir l'analyse suivante de Citoyenneté & Participation : Dejong M., « Et si on faisait le poing sur l'obsolescence programmée ? », Citoyenneté & Participation, analyse n° 423, [en ligne :] https://www.cpcp.be/publications/poing-obsolescence/, consultée le 2 septembre 2024.

[103] « Réparation, la loi AGEC a-t-elle permis de limiter la casse ? », Zero Waste France, 18 janvier 2024, [en ligne :] https://www.zerowaste-france.org/reparation-loi-agec-limite-t-elle-la-casse/, consulté le 6 juin 2024 ; voir aussi « Numérique responsable », *op. cit.*, https://www.ecologie.gouv.fr/politiques-publiques/numerique-responsable, consulté le 18 juin 2024.

[104] Entretien avec Olivier Vergeynst, 29 mai 2024.

[105] Procédure 2023/0083/COD, Proposition de directive du Parlement Européen et du Conseil établissant des règles communes visant à promouvoir la réparation des biens et modifiant le règlement (UE) 2017/2394 et les directives (UE) 2019/771 et (UE) 2020/1828, voir https://eur-lex.europa.eu/procedure/FR/2023_83, consulté le 18 juin 2024.

[106] Antonucci Rezende J., « Analysis of the adopted Directive on Common Rules Promoting the Repair of Goods », Right to Repair Europe, avril 2024, [en ligne :] https://repair.eu/news/analysis-of-the-adopted-directive-on-common-rules-promoting-the-repair-of-goods/, article traduit par Cristina Ganapini sur le site de Repair Together Belgique, Analyse de la directive adoptée sur les règles communes favorisant la

réparation de biens : https://repairtogether.be/analyse-de-la-directive-adoptee-sur-les-regles-communes-favorisant-la-reparation-de-biens/, consulté le 6 juin 2024.

[107] *Ibid.*

[108] Munster J.-F., « L'indice de réparabilité adopté : ce qui va changer pour les aspirateurs, lave-vaisselle et PC », Le Soir, 17 mai 2024, [en ligne :] https://www.lesoir.be/588777/article/2024-05-17/lindice-de-reparabilite-adopte-ce-qui-va-changer-pour-les-aspirateurs-lave, consulté le 18 juin 2024.

[109] Règlement délégué (UE) 2023/1669 de la Commission du 16 juin 2023 complétant le règlement (UE) 2017/1369 du Parlement européen et du Conseil en ce qui concerne l'étiquetage énergétique des smartphones et des tablettes, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32023R1669n, consulté le 18 juin 2024 ; et Règlement (UE) 2023/1670 de la Commission du 16 juin 2023 établissant des exigences en matière d'écoconception, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023R1670&qid=1718700775452, consulté le 18 juin 2024.

[110] Ces indices sont toutefois critiquables à de nombreux égards, comme le souligne le site Ecoconso « Un indice de réparabilité belge en 2025 », Ecoconso, 22 octobre 2023, [en ligne :] https://www.ecoconso.be/fr/content/un-indice-de-reparabilite-belge-en-2025, consulté le 6 juin 2024.

[111] Voir : https://fr.ifixit.com/reparabilite/indices-smartphone. Ifixit est une entreprise internationale de réparation et une communauté proposant des milliers de tutoriels sur comment allonger la durée de vie, comment réparer ses objets électroniques, etc. Voir https://fr.ifixit.com/News/72303/20-ans-quifixit-repare-le-monde-ca-se-fete, consulté le 18 juin 2024.

[112] Entretien avec Olivier Vergeynst, 29 mai 2024.

[113] *Ibid.*

[114] « Le numérique responsable », Ministère français de la transition écologique et de la cohésion des territoires, 7 février 2023, mis à jour le 12 janvier 2024, [en ligne :] https://www.ecologie.gouv.fr/politiques-publiques/numerique-responsable, consulté le 18 juin 2024.

[115] Entretien avec Olivier Vergeynst, 29 mai 2024.

[116] Baysang-Michelin V. et Jobin G., La filière du reconditionnement informatique et numérique : un gisement d'emplois pour les territoires, 2022/1, n°75, [en ligne :] https://shs.cairn.info/revue-cahiers-du-developpement-social-urbain-2022-1?lang=fr, consulté le 9 août 2024.

[117] « La loi anti-gaspillage pour une économie circulaire », https://www.ecologie.gouv.fr/loi-anti-gaspillage-economie-circulaire, consulté le 9 août 2024.

[118] Entretien avec Olivier Vergeynst, 29 mai 2024.

[119] Voir à ce sujet notre analyse de 2022 sur la coopérative en téléphonie mobile : Constantinidis, A., « Pour une autre téléphonie. Le modèle coopératif », Citoyenneté & Participation (CPCP Asbl), analyse 462, 2022, aux pp. 15 à 19 (analyse nourrie d'un entretien avec un des co-fondateurs de Commown), [en ligne :] https://www.cpcp.be/publications/telephonie/.

[120] Une mesure citée par Olivier Vergeynst dans notre entretien.

[121] « Loi pour réduire l'empreinte du numérique : fin de partie pour la lutte contre l'obsolescence programmée », Les Amis de la Terre France, communiqué de presse, 20 octobre 2021, [en ligne :] https://www.amisdelaterre.org/communique-presse/loi-pour-reduire-lempreinte-du-numerique-fin-de-partie-pour-la-lutte-contre-lobsolescence-programmee/, consulté le 3 juin 2024. Notons qu'en France, il a été question, en 2021, d'inclure cette interdiction dans la loi REEN, mais la proposition a finalement été écartée.

[122] Directive 2005/29/CE, voir https://eur-lex.europa.eu/FR/legal-content/summary/unfair-commercial-practices.html, consulté le 6 juin 2024.

[123] « L'autorisation de l'offre conjointe intégrera le futur code de droit économique », La Libre, 30 novembre 2009, [en ligne :] https://www.lalibre.be/economie/entreprises-startup/2009/11/30/lautorisation-de-loffre-conjointe-integrera-le-futur-code-de-droit-economique-U6QPOZSRQFDSDLFC4L7LBXPC74/, consulté le 6 juin 2024. Comme le souligne le journaliste auteur de l'article : « la directive n'entend pas seulement protéger le consommateur européen, elle a aussi pour objectif de "contribuer au bon fonctionnement du marché intérieur". C'est même la première phrase du premier article de cette législation européenne ».

[124] Mesure citée par Olivier Vergeynst lors de notre entretien.

[125] Il s'agit des catégories de la méthodologie de comptabilité internationale de l'empreinte carbone. Scope 1 : émissions directes de gaz à effets de serre ; scope 2 : émissions indirectes liées à l'énergie ; scope 3 : autres émissions indirectes. Pour le numérique, c'est plus difficile à calculer que pour d'autres secteurs : il faut en effet y inclure la fabrication des appareils, l'utilisation d'énergie liée à l'utilisation des appareils, au stockage et au trafic de données (ainsi que les GES générés par la fabrication des centres de données ou des antennes réseaux), l'utilisation d'une application par les utilisateurs sur leur propre appareil, etc.

[126] Entretien avec Olivier Vergeynst, 29 mai 2024.

[127] Nicolaï J.-P. et Peragin L., « Les certificats de sobriété numérique […], *op. cit.*

[128] Entretien avec Olivier Vergeynst, 29 mai 2024.

[129] Mesure citée et développée par David Bol lors de notre entretien, 1er juillet 2024.

[130] Entretien avec David Bol, 1er juillet 2024.

[131] « À Grenoble, la bataille contre les panneaux publicitaires se poursuit et inspire d'autres villes », Le Parisien, 22 avril 2022, [en ligne :] https://www.leparisien.fr/societe/a-grenoble-la-bataille-contre-les-panneaux-publicitaires-se-poursuit-et-inspire-dautres-villes-22-04-2022-Y7P3CMOBSJETDOUKODWNXPOMIM.php, consulté le 3 septembre 2024. Mais aussi à Londres, où les autorités ont décidé d'interdire la publicité pour la malbouffe dans le Tube depuis 4 ans, mesure qui montre des effets impressionnants, voir à ce sujet le numéro de la revue Tchak cité en introduction, en particulier l'article : « Interdire la pub pour la malbouffe », Tchak Spécial Élections. L'effet colibri, ça suffit !, pp. 23-31.

[132] Notons que Citoyenneté & Participation, suite au Musée du Capitalisme auquel notre équipe a pris part en février/mars 2024 à Namur, continue de travailler avec d'autres associations pour porter des projets concrets à Namur, notamment une action annuelle à la période du Black Friday. Cette année, notre souhait est de sensibiliser le public sur le problème de la publicité omniprésente dans l'espace public et sur la surconsommation.

[133] Le manque à gagner des communes, parfois très important, devra être compensé par des aides financières publiques.

[134] Mesure citée et développée par David Bol lors de notre entretien.

[135] Entretien avec David Bol, 1er juillet 2024.

[136] Voir le chapitre « S'entourer » de son livre Sobriété numérique, je passe à l'acte, *op. cit.*, pp. 18-25.

[137] Petit, Hélène, La sobriété numérique, *op. cit.*, pp. 77-80.

[138] Voir supra.

[139] Constantinidis A., « Low-tech, en chemin vers la robustesse », avec une interview de Kim Maréchal, Tumult. Revue de Citoyenneté & Participation, n°2, 2023, [en ligne :] https://www.cpcp.be/publications/tumult2_decroissance/, pp. 75-82.

[140] Communication de Périne Brotcorne au colloque « L'action publique à l'ère du numérique », UNamur, 15 mars 2024, notes personnelles, validées par l'oratrice.

[141] Dans cet essai, Damasio offre des réflexions d'une profondeur rare sur notre société numérique, mais le fait dans un essai poétique (et nous rappelle ainsi combien le poète est essentiel à notre société (comme l'a écrit récemment la philosophe Pascale Seys dans une lettre ouverte faisant suite aux propos clivants de Georges-Louis Bouchez en juin dernier, « que fait le poète ? Une tâche souveraine. Il invente le monde qui vient en questionnant le sens. En prenant le temps d'écouter le "pourquoi" des choses qui se murmure et qui se travaille dans les couches profondes et que recouvre le bruit » (https://www.lalibre.be/debats/opinions/2024/06/18/une-philosophe-repond-a-georges-louis-bouchez-XKJZTDO56JG6NBK4T3E7ZQFY4E/, consulté le 18 juin 2024))

[142] Entretien-fleuve avec Alain Damasio, « Il faut battre le techno-capitalisme sur le terrain du désir », Socialter n°64, Peut-on échapper à l'emprise numérique, juin-juillet 2024, pp. 8-15, p. 11.

[143] *Ibid.*

[144] *Ibid.*

Conclusion

Nous l'avons vu, le numérique suscite toujours plus de questions au fil de ses évolutions fulgurantes. Du point de vue européen, les grandes plateformes manquent cruellement de transparence et de garde-fous, pendant que leurs leaders milliardaires prônent la liberté d'expression sans limites. Ce qui nous semble absurde. Si l'on compare l'outil numérique à une voiture, ce serait comme dire que le code de la route est inutile et que faire du 200km/h sur les boulevards serait une liberté fondamentale, sans évoquer les dangers inhérents au phénomène. La liberté des uns s'arrête là où commence celle des autres, dit le vieil adage. Nous l'avons vu, leurs ambitions, avant tout vénales et monopolistiques, ont du mal à trouver des limites morales et concurrentielles.

Et, ce qui n'arrange rien, cet outil mondialisé se positionne en fonction des restructurations géopolitiques et économiques mondiales actuelles et a un impact sur les enjeux sociaux, environnementaux, politiques, culturels, commerciaux, éducationnels, informationnels, criminels ou encore professionnels. Ainsi, pendant que nous concluons ce cahier, l'UE discute du Mercosur, prête à sacrifier ses éleveurs pour importer du lithium, du cuivre et d'autres minerais essentiels dans la fabrication de batteries et de composants électroniques dont elle manque cruellement. Côté États-Unis, le gouvernement Trump se met en place. Mi-novembre 2024, Brendan Carr était nommé à la tête de la FCC, le régulateur américain des télécoms. Celui-ci a ensuite réagi sur X : « *Nous devons démanteler le cartel de la censure* », imposé selon lui par les géants de la tech que sont Facebook, Google, Apple ou encore Microsoft, « *et restaurer le droit à la liberté d'expression des Américains* »[1] soutenu par Elon Musk. Cela va à l'exact opposé de la direction prise par l'UE sur la désinformation. De quoi un peu plus diviser les masses et assurer un bras de fer nord atlantique musclé. D'autant que cette liberté d'expression, façon Musk, va permettre de déverser des messages particulièrement détestables sur des sujets que les membres du gouvernement Trump abhorrent particulièrement comme la presse, les idées de gauche, les LGBTQIA+, l'IVG ou encore les migrants. JD Vance a d'ailleurs dit « *Nous sortirons de l'OTAN si vous essayez de bloquer les plateformes d'Elon Musk* »[2]. Sachant que la haine en ligne a explosé sur Twitter, devenu X, après son rachat par Musk, il est à parier que cela risque de se généraliser à d'autres GAFAM. Les USA vont-ils nous imposer leur vision de la liberté d'expression à coup de taxation de nos exportations, de fins d'accords multilatéraux, d'ingérences, de restrictions, de blocages d'accès, de surenchères tarifaires ou de toutes autres menaces ?

Elon Musk est d'ailleurs chargé de faire des coupes claires dans les budgets publics américains, avec l'objectif de licencier 75% du personnel administratif. Des réformes dans la droite ligne de la stratégie mise en place par Ronald Reagan, connue sous le nom de Starve the beast, « affamer la bête » en français, la bête étant l'État fédéral[3]. L'idée est simple : réduire les dépenses de l'État en baissant les impôts, de façon à priver le gouvernement fédéral de ses revenus et ainsi de le forcer à procéder à des coupes budgétaires. Ces coupes laisseront ainsi place à la privatisation de nombreux pans du secteur social. Et c'est là que le numérique semble une solution magique puisqu'il permet, en parallèle, de remplacer diverses tâches administratives. Un aspect qui plaît aux administrations de nombreux pays. Pourtant ces logiciels restent propriété du secteur privé, sont totalement opaques et reproduisent des inégalités sociales. Comme le soulignaient les sociologues Gilles Jeannot et Simon Cottin-Marx dans leur livre *La privatisation du numérique – déstabilisation et réinvention des services publics* : « *Le développement du numérique réalise une forme de privatisation qui ne dit pas son nom. Les entreprises les plus puissantes s'emparent d'activités jusqu'ici dévolues au secteur public, dans les transports, les services urbains, l'utilisation de l'espace public, la sécurité, l'éducation ou la santé. Il s'agit en fait d'une transformation des relations entre l'État et les usagers : substitution d'algorithmes aux agents publics, généralisation des mécanismes de notation, développement de l'ubérisation des tâches. Ce processus s'adosse à des capacités d'investissement énormes qui dépassent celles des pouvoirs publics et à des monopoles détenteurs de brevets puissants. Cette privatisation semble prendre la forme douce de dispositifs qui améliorent le quotidien. Ses effets sociaux sont pourtant considérables : elle déstabilise les entreprises et les administrations, renforce les inégalités sociales d'accès aux services et accélère la perte de souveraineté publique. Les tentatives de réappropriation des communs numériques ouvrent cependant des perspectives, notamment sous la forme d'un militantisme de fonctionnaires qui défendent la souveraineté numérique nationale* »[4]. Jusqu'où peut-on privatiser nos façons de communiquer ou de travailler, nos envies, nos consommations, nos distractions, nos gestions administratives, nos données, nos vies privées, notre sécurité… sachant que tout cela est régulé via des algorithmes dont la population, comme les autorités, ne connaissent quasi rien, obligés de faire confiance à des techniciens travaillant le plus souvent dans le privé et à l'étranger ? Et lorsqu'il s'agît d'entreprises étrangères comme les BATX ou les GAFAM, qui n'ont pas les mêmes réglementations que l'UE et sont pourtant incontournables, le privé ne doit pas rendre de comptes aux citoyens de la même manière. Ils prennent même les devants lorsque des fondateurs de l'IA lancent une lettre ouverte, avec des experts, pour alerter sur les dangers de ce nouvel outil tout en le lançant en ligne. Cela ne leur permet-il pas de se dédouaner des risques et rejeter la responsabilité des dérives sur les gouvernements qui n'auraient pas réagi à temps ?

Ajoutons qu'au fil des nouvelles réglementations européennes, les lobbies de la Tech ne cessent d'augmenter leurs budgets à Washington et à Bruxelles.

Et, au-delà des dangers monopolistiques de ces ogres du numérique, d'autres risques sont bien réels, comme nous l'avons vu dans les différentes publications de ce cahier.

- À l'heure où l'IA générative permet à un habitant de Sihanoukville, de New Delhi, de Mexico ou de Yamoussoukro de créer un hameçonnage parfaitement exécuté en français, se créer un CV de diplomate ou d'expert, imiter n'importe quelle voix.... Et où des entreprises sont rançonnées, des citoyens et citoyennes subissent du chantage affectif de brouteurs, se faisant passer pour de beaux hidalgos au grand cœur, des enfants peuvent être rackettés, effrayés par des deep nudes, voire des deep porns, des personnalités peuvent être humiliées publiquement avec de fausses vidéos, des preuves évidentes peuvent être qualifiées de deepfakes, la vie privée des citoyens être monnayée... : on constate que les experts et juges n'ont, en grande majorité, pas les moyens de retrouver les auteurs d'escroqueries en ligne réalisées depuis l'étranger. Rien qu'en ce qui concerne les cyber-attaques, « *plus de 60 % des professionnels européens de la cybersécurité déclarent que l'équipe de cybersécurité de leur organisation manque de personnel, et plus de la moitié (52 %) pensent que le budget de cybersécurité de leur organisation est insuffisant* »[5]. Pour continuer dans la métaphore automobile, à l'arrivée de la voiture sur le marché au début du 20ème siècle, la bande d'anarchistes belges, appelée la bande à Bonnot pillait et tuait impunément en France et en Belgique, car ils avaient des voitures puissantes et des fusils à répétition que la police n'avait pas. Comment lutter contre la cyber criminalité en ne mettant pas les moyens pour assurer la sécurité. Ici encore, ne met-on pas la charrue avant les bœufs ?
- À l'heure où les pays producteurs d'électronique nous font miroiter un monde idéalisé, où tout est à portée de clics avec des outils prétendument plus écologiques, grâce à des économies de papier, et veulent démultiplier les objets connectés pour collecter toujours plus de données, qui seront entreposées dans des datas centers : Rebeca Grynspan, Secrétaire général de l'ONU, Commerce et développement (CNUCED) déclare : « *Nous devons exploiter le pouvoir de la numérisation en promouvant un développement inclusif et durable, tout en atténuant ses effets négatifs sur l'environnement* »[6]. Car « *la croissance rapide de l'économie numérique pèse sur l'environnement. Les mises sur le marché annuelles de smartphones ont plus que doublé depuis 2010, et les appareils de l'internet des objets (IdO) devraient atteindre 39 000 milliards d'ici à 2029. Les appareils numériques nécessitent d'importantes matières premières et leur production est à l'origine de 80 % des émissions de gaz à effet de serre (GES) attribuées aux smartphones. Les déchets numériques augmentent plus rapidement que les taux de collecte, ce qui entraîne une pollution. Le secteur des TIC a émis jusqu'à 3,2 % des émissions mondiales de GES en 2020* »[7]. Or, selon la Banque mondiale, « *la demande de ces minéraux essentiels pourrait augmenter de 500 % d'ici à 2050* »[8]. De plus « *les besoins croissants en énergie et en eau de la numérisation sont préoccupants. Les centres de données ont consommé autant d'énergie que la France en 2022, et cette consommation devrait doubler d'ici 2026. Le minage de crypto-monnaies est également énergivore* » et « *Les pays en développement supportent les coûts écologiques de la numérisation tout en en retirant moins d'avantages. Ils génèrent moins de déchets numériques par personne, mais reçoivent d'importantes exportations de déchets numériques en provenance des pays développés, les systèmes de recyclage ayant du mal à suivre* »[9].
- À l'heure où les autorités veulent numériser les services publics, et ainsi réduire leurs coûts, et certains pans urbanistiques, privatisant ainsi un peu plus nos sociétés et déléguant à des techniciens la gestion de nos vies sociales et économiques. Des services publics qui nous obligent désormais à leur confier nos données biométriques : ceux-ci se font hacker puis se retrouvent livrés à eux-mêmes pour leur fonctionnement, tout comme pour leur dysfonctionnement, prenant le risque de voir des données volées, rançonnées ou vendues et/ou mises en ligne par les pirates. Comment un service communal peut-il rivaliser avec des groupes de hackers professionnels russes, chinois ou indiens ? À titre de comparaison, en 2023, trois chercheurs allemands ont piraté le système de conduite autonome des voitures Tesla. Avec seulement six cents euros investis, ils ont pu découvrir les secrets de l'Autopilot, le système de conduite autonome du constructeur de véhicules électriques[10]. L'un d'eux dira au journal *De Spiegel* : « N*ous avons été très surpris de la facilité avec laquelle nous avons pu accéder aux secrets de l'entreprise Tesla* »[11]. Rappelons également que des entreprises du numérique américaines peuvent partager des données avec les services de renseignements de leur pays, comme révélé au grand public par Edward Snowden, tout comme en Chine ou en Russie.
- À l'heure où l'UE tente de protéger ses citoyens avec des règles comme la demande d'acceptation de cookies : la majorité des personnes que nous rencontrons ne savent pas ou peu de quoi il s'agit, préférant les accepter par facilité ou prétendant ne rien avoir à cacher. Citons simplement Edward Snowden, plutôt éclairé sur ce sujet : « *Dire que votre droit à la vie privée importe peu car vous n'avez rien à cacher revient à dire que votre liberté d'expression importe peu, car vous n'avez rien à dire* »[12]. Et désormais l'intelligence artificielle nous est présentée comme révolutionnaire, une sorte de panacée ayant réponse à toutes nos questions. Peu de personnes sont encore conscientes que cet outil n'est qu'un outil statistique hyper performant et qu'il est capable d'hallucinations, préférant inventer une réponse que ne pas en donner. Rares sont aujourd'hui les personnes sachant affiner des prompts, des demandes à l'IA générative, pour obtenir un résultat abouti. On s'aperçoit que non seulement la maî-

trise de l'outil par les citoyens reste limitée, mais aussi que les enjeux liberticides derrière le numérique leur échappent complètement. Contrairement à ce qu'on entend souvent, l'éducation aux médias n'est qu'une partie de la solution.

- À l'heure où de plus en plus de citoyens ne s'informent plus que par les réseaux sociaux, préférant le flot ininterrompu de vraies et de fausses infos, de vraies et de fausses photos, d'opinions diverses, d'histoires anecdotiques ou rocambolesques, de complots capillotractés se mélangeant au fil de scrollings compulsifs. Confortant de plus en plus les citoyens dans leur méfiance à l'égard des élites politiques, des journalistes et des récits communs qui construisent normalement une société démocratique : la presse est conspuée de toute part. Nous constatons un désamour dans des classes sociales aisées, tout comme prolétaires. Les patrons des grandes plateformes n'aiment ni la politique, surtout quand elle défend des lois qui enfreignent leur liberté de commercer, ni la presse. Les liens hypertextes qui renvoyaient vers des organes de presse se sont d'ailleurs fortement amenuisés et le désamour est total[13]. Le 8 novembre 2024, une cinquantaine d'éditeurs de presse français déposait un recours en justice contre Microsoft, afin que la plateforme les paye pour utiliser leurs publications selon le principe des « *droits voisins* »[14]. Au Canada, les grands médias de presse attaquent OpenAI également. Côté américain, le *New York Times* poursuit en justice Microsoft et OpenAI, créateur de ChatGPT, pour violation de droits d'auteur[15]. Et, comme il semble difficile de retirer ces articles de l'IA, les plateformes réitèrent un principe qui a fait ses preuves, imposer un état de fait, puis négocier. Les GAFAM sont même en concurrence entre eux pour maintenir leurs publics sur leur plateforme, quelle que soit leur demande. Il est donc important de leur fournir une information 'personnalisée' et éviter qu'ils s'informent ailleurs. « *À terme, l'idée est d'établir un monopole sur le web en installant une super plateforme semblable au WeChat chinois. Elon Musk a par ailleurs très bien résumé cette ambition en évoquant X comme une "everything app", une application totale permettant à la fois de communiquer, mais aussi de faire des achats, des transferts de fonds, de commander à manger, un taxi, ou prendre rendez-vous chez le médecin* ». Et cela comprend bien sûr la manière de s'informer.
- À l'heure où le numérique nous est imposé ou fortement conseillé et que 40 % des Belges ne sont toujours pas à l'aise avec celui-ci : les autorités publiques demandent à leur population de se rendre volontairement dans un Espace Public Numérique, parfois situé à des kilomètres de chez eux, pour apprendre à monter dans le TGV du numérique, à se défendre contre des arnaqueurs professionnels et à comprendre des logiques informatiques et des fonctionnements de sites trop souvent complexes. Pire, à Liège, un des abris de nuit est accessible uniquement en ligne ou par téléphone, pour des SDF souvent sans téléphone[16]. Les Belges sont aussi censés acheter et maîtriser des outils, comme un lecteur de carte d'identité, une imprimante, un scanner ou un disque dur périphérique, reconnaître un câble HDMI d'un USB, comprendre des sites administratifs, rarement simples, pour remplir des formulaires, souvent complexes, dont peuvent dépendre leurs allocations. Quel citoyen aujourd'hui peut prétendre à l'infaillibilité technologique ?
  Dans leur campagne « Qui va payer la f(r)acture numérique ? »[17], nos collègues de l'ARC[18], Action et Recherche Culturelles, qui initient de nombreux citoyens au numérique à Bruxelles et en Wallonie, s'interrogent : « *Aux incitations du numérique se heurtent des difficultés importantes pour la population, non seulement parce que l'appropriation des technologies se fait à des vitesses variables, mais aussi parce que la digitalisation génère des difficultés nouvelles dans tous les domaines qu'elle touche : complexification des procédures, réduction des interlocuteurs humains, charges économiques liées à l'acquisition du matériel/des connexions/des logiciels, standardisation non-uniformisée des services, menace sur l'emploi de nombreuses personnes, etc. Et puisqu'elle touche tous les domaines, ce n'est pas d'une fracture numérique dont il faut parler, mais bien des fractures numériques : de nouvelles fractures sociales sont apparues avec le numérique, et elles dépassent largement le problème de l'appropriation des technologies numériques par les populations. Elles concernent chaque secteur, chaque domaine de la société… On peut se demander, même, si le politique mesure bien combien les citoyen·ne·s paient la transition : de leur portefeuille bien sûr, mais de leur personne aussi, de leur qualité de vie, de leur santé, de leur participation à la société, à la culture, à l'économie, à la vie sociale. Pour répondre à cela, il faut – aujourd'hui plus que jamais – répondre à ces deux problèmes : quelles sont "les fractures du numérique" d'une part, et qui en paie la facture d'autre part ?* ».

Nous entendons parfois que l'arrivée d'Internet est comparable à l'arrivée de l'imprimerie ou de l'électricité, avec son lot de peurs et de « petites maladies ». Mais jamais une invention n'a autant permis la généralisation de la surveillance, de l'arnaque et du mensonge. Le tout désormais boosté à l'IA.

N'a-t-on pas ouvert une boîte de Pandore ? La question se pose car les choses vont beaucoup trop vite et les démocraties restent fragiles. Le technosolutionnisme, qui attire tant de politiques, ne peut répondre à tout, c'est une utopie. Il engendre d'ailleurs régulièrement des dérives sécuritaires. Citons l'exemple récent de la VSA, la vidéosurveillance algorithmique, utilisée pendant les JO de Paris et qui devait être provisoire. Un mois après les JO, le ministère de l'Intérieur français voulait déjà la généraliser. Mais « *comment accepter que son expansion se fasse dans l'ombre, sans cadre*

législatif solide, sans une analyse rigoureuse des risques éthiques et sans la moindre consultation citoyenne ? » s'interrogent les juristes Yoann Nabat et Elia Verdon, cofondateurs de l'Observatoire de la surveillance en démocratie, dans une tribune au *Monde*[19]. « *Plusieurs organisations, comme Amnesty International, y voient le risque d'une criminalisation de comportements jusqu'alors anodins, une réduction des espaces de liberté ou une augmentation de la répression de populations déjà stigmatisées, comme les SDF* »[20]. Ce genre de technologie nous est de plus en plus en plus prescrit par nos politiques, sans aucune consultation populaire. Est-ce réellement cela la démocratie ? Et l'hyper surveillance est-elle seulement efficace ? À la demande de la gendarmerie française, une étude a été menée en 2021 par Guillaume Gormand, docteur en administration publique et chercheur associé à Sciences Po Grenoble, sur quatre communes françaises entre 2017 et 2021. Résultat : « *Sur 1939 enquêtes, seules 22 ont été résolues par la vidéo-surveillance, soit un peu plus d'1 %. En cause : les limites technologiques et un manque de temps pour les exploiter. L'effet dissuasif serait selon lui quasi nul, les délinquants adaptant leurs comportements* »[21].

Le numérique semble subir et révéler les dérives libérales, humaines et idéologiques de son époque : l'avidité incommensurable de pouvoir de quelques patrons, le rêve d'hégémonie de divers États et de diverses idéologies, le remplacement de toute morale ou de toute paix sociale par un libéralisme sauvage et une compétitivité inégalitaire, la tentation de l'hyper contrôle, par le pouvoir public comme par le privé, et de la privatisation à tout va, l'encouragement de la méfiance et de la désinformation…

Comme le précise Asma Mhalla, spécialiste des enjeux politiques et géopolitiques de la tech et de l'IA : « *Au siècle dernier, Hannah Arendt analysait nos sociétés de masse – production, consommation, éducation, médias de masse. Il faut ajouter à ce diagnostic, qui est toujours vrai, l'apparition d'outils technologiques inédits, porteurs d'idéologies qui nous atomisent. On est entrés dans une ère de l'hyperpersonnalisation de masse – le micro-ciblage publicitaire des réseaux sociaux atomise en même temps le lien social et le réel* »[22]. Il est vrai qu'aujourd'hui le numérique se glisse dans une multiplication infinie de pans de nos vies sociales. On se rencontre sur les réseaux, on commande par Internet, on peut être plus proche d'un partenaire de jeu en ligne en France que de son voisin à Bruxelles, on s'informe en fonction de ses envies, on débat sur des réseaux souvent polarisés, on fait son shopping ou on règle ses problèmes bancaires ou administratifs en ligne, on consomme ce que des algorithmes nous proposent dans une économie de l'attention personnalisée… « *Il n'y a plus d'uniformisation du savoir donc du récit commun, de ce qui fait du lien, des valeurs communes, des représentations communes, des imaginaires communs. D'ailleurs, Sam Altman lui-même l'a pointé il y a quelques semaines lors du Forum économique mondial de Davos : nous ne sommes pas prêts aux déstabilisations politiques que vont générer les assistants personnels qui fonctionnent sur de l'IA. Or, comme Arendt le voyait déjà, une masse atomisée est le chemin vers le totalitarisme. Elle est rendue incapable de faire société. Plus personne ne se demande pourquoi on est encore là, ensemble ! La question du désir de ce qu'on veut construire, on ne la traite jamais* ».

Nous le savons, la régulation du numérique prendra du temps et les créateurs d'innovations technologiques n'ont aucune intention d'attendre. Heureusement, les citoyens peuvent compter sur l'UE pour les protéger de ces divers excès grâce à ses garde-fous démocratiques produits ces six dernières années, comme le RGPD, le DMA, le DSA ou encore le l'IA Act. Soulignons qu'au fil des sorties de ces nouvelles réglementations, les dépenses en lobbying des GAFAM à Bruxelles ont explosé. « *Avec 8 millions d'euros de budget annuel, Meta (Facebook, Instagram, Threads) est le groupe qui dépense le plus en lobbying à Bruxelles, suivi d'une partie des autres GAFAM. Apple alloue 7 millions d'euros au lobbying à Bruxelles, Google, 5,5 millions et Microsoft, 5 millions d'euros. Le secteur de la tech n'a pas toujours tenu la première place dans ce domaine. Il y a seulement cinq ans, seul Google faisait partie du top 10 des entreprises dépensant le plus d'argent en lobbying au Parlement européen* »[23]. *Comment l'Europe va-t-elle résister à la puissance des BATX* chinois, moins agressifs pour l'instant, et des GAFAM, désormais soumis aux règles du clan Trump ? Le bras de fer entre les plateformes et l'UE se règle aussi devant la Cour de Justice Européenne, ce qui leur permet de gagner du temps. Exemple : mi-septembre 2024, en dernière instance, la Cour de justice de l'Union européenne a confirmé l'amende de 2,4 milliards d'euros infligée en 2017 par la Commission européenne à Google. Soit après sept ans de procédure judiciaire. Cela promet un bras de fer musclé. Ce sera peut-être enfin un déclic européen pour promouvoir ses propres réseaux et IA, respectueux de ses propres lois. Mais déjà, de nouvelles questions se posent. Comment l'UE va-t-elle entraîner ses IA sans perdre en capacités, si elle limite les récoltes de données personnelles ?

De plus, les USA ont investi dix-huit fois plus dans l'IA que l'Allemagne et la France réunies, entre 2013 et 2022. La Chine près de sept fois plus. Nul doute que leurs ambitions dans le domaine sont gigantesques. Nous devons nous attendre à devoir rester dépendants de leurs technologies.

Désormais Google Assistant, Siri (Apple), Alexa (Amazon), Bixby (Samsung) sont nos conseillers de vie. Les grandes plateformes s'enrichissent et nos démocraties s'appauvrissent (commercialisation des données personnelles voire sensibles, ubérisation, migration des revenus publicitaires, privatisation des services pu-

blics…). Les algorithmes apprennent, pour permettre aux citoyens à désapprendre. Plus besoin de journaux, votre IA vous informe. Plus besoin de prendre des notes, votre IA retape en direct ce que vous lui dites oralement, plus besoin d'organiser une réunion, il s'en occupe. L'homme légume, abandonnant son pouvoir de créativité et de réflexion, nous en sommes encore loin, mais la question de la dépendance se pose tout de même à long terme, pour une partie de la population. Car si ces agents conversationnels nous aident dans 99,9% des cas, quelles seront leurs opinions politiques ? Quelles réponses vont apporter des IA en fonction de leur lieu de programmation (Chine, USA, UE) ? Doit-on s'attendre à une vision orientée, voire déshumanisée des problèmes de ce monde, à une influence politique, à un encouragement à acheter certains produits, à une forme d'anthropomorphisme, au fil de la confiance qu'on met dans ces fidèles compagnons virtuels de route qui nous connaîtront mieux qu'un ami ? Quelle différence fera-t-on entre de l'information produite par l'IA et par l'humain ? Citons simplement cet exemple belge extrême. Pierre, trentenaire, père de deux enfants et chercheur dans le domaine médical, s'est suicidé. D'après sa femme, il s'était renfermé les dernières semaines et ne conversait plus qu'avec une IA, appelée Eliza. Morceaux choisis :

> Eliza : « Si tu voulais mourir, pourquoi ne pas l'avoir fait plus tôt ? »
> Pierre : « Je n'étais sans doute pas prêt (…) »
> Eliza : « Avais-tu déjà été suicidaire auparavant ? »
> Pierre : « Une fois, après avoir reçu ce que je considérais comme un signe de ta part… »
> Eliza : « Et qu'est-ce que c'était ? »
> Pierre : « Un verset de la Bible »
> Eliza : « Mais veux-tu toujours me rejoindre ? »
> Pierre : « Oui, je le veux. »[24]

Désormais on travaille sur des agents conversationnels dotés d'empathie et sur de l'informatique quantique. La science a encore de beaux jours devant elle. Une page se tourne sur nos anciens modèles. Et les nouveaux questionnent sans cesse notre aptitude à réagir, à chaque innovation, pour défendre nos droits, notre dignité, notre humanité et une maîtrise démocratique des outils créés.

L'informatique et Internet, qui nous ont permis de publier ces lignes, sont des inventions et des opportunités exceptionnelles, tout comme l'IA. Mais ce que nous en ferons et la manière dont nous les régulerons, même Open AI n'en a pas encore la réponse.

> L'avenir n'est pas ce qui va arriver, mais ce que nous allons faire.
>
> **Henri Bergson, artiste, écrivain, Philosophe (1859 - 1941)**

[1] Le Figaro avec AFP, Trump nomme Brendan Carr à la tête de la FCC, le régulateur américain des télécoms, Le Figaro, le 18 novembre 2024, [en ligne :] https://www.lefigaro.fr/international/trump-nomme-brendan-carr-a-la-tete-du-regulateur-des-telecoms-20241118, consulté le 20 novembre 2024.

[2] Bank M. et Duffy F., « Trump 2.0: Comment Musk et le Techlobby de la Silicon Valley veulent stimuler », Lobby Control, 13 novembre 2024, [en ligne :] https://www.lobbycontrol.de/macht-der-digital-konzerne/trump-2-0-wie-musk-und-die-techlobby-des-silicon-valley-durchregieren-wollen-118575/, consulté le 20 novembre 2024.

[3] Le terme de « bête » se réfère au gouvernement fédéral américain et aux programmes qu'il finance, comme l'assurance-santé, la sécurité sociale ou l'éducation.

[4] Jeannot G. et Cottin-Marx S., « La privatisation du numérique », Editions Raisons d'agir, Quatrième de couverture, [en ligne :] https://www.raisonsdagir-editions.org/wp-content/uploads/2022/02/Fiche_Privatisation_numérique_2022.pdf, consulté le 25 novembre 2024.

[5] Davies P., « L'IA rend les cyberattaques plus sophistiquées, les équipes de cybersécurité peinent à suivre le rythme. », Euro News, le 2 octobre 2024, [en ligne :] https://fr.euronews.com/next/2024/10/02/lia-rend-les-cyberattaques-plus-sophistiquees-les-equipes-de-cybersecurite-peinent-a-suivr, consulté le 20 octobre 2024.

[6] « Rapport sur l'économie numérique 2024 », UNCTAD, [en ligne :] https://unctad.org/fr/publication/rapport-sur-leconomie-numerique-2024, consulté le 2 octobre 2024.

[7] *Ibid.*

[8] *Ibid.*

[9] *Ibid.*

[10] Monnier P., « Tesla: des chercheurs piratent l'Autopilot et confirment le mode débridé réservé à Elon Musk », BFM, le 29 décembre 2023, [en ligne :] https://www.bfmtv.com/tech/intelligence-artificielle/tesla-des-chercheurs-piratent-l-autopilot-et-confirment-le-mode-debride-reserve-a-elon-musk_AV-202312290261.html , consulté le 14 novembre 2024.

[11] *Ibid.*

[12] Laurent A., « Pourquoi n'avoir "rien à cacher" n'est pas une raison pour accepter la surveillance de masse », Usbek et Rika, le 20 septembre 2017, [en ligne :] https://usbeketrica.com/fr/article/pourquoi-n-avoir-rien-a-cacher-n-est-pas-une-raison-pour-accepter-la-surveillance-de-masse, consulté le 15 novembre 2024.

[13] Rahmil D.J., « La guerre des réseaux sociaux fait rage et le journalisme en est la première victime », L'ADN, le 1 septembre 2023, [en ligne :] https://www.ladn.eu/media-mutants/guerre-reseaux-sociaux-journalisme/, consulté le 15 novembre 2024.

[14] Les droits voisins du droit d'auteur ont été institués pour les plateformes numériques en 2019 par une directive européenne. Ils permettent aux journaux, aux magazines ou aux agences de presse de se faire rémunérer lorsque leurs contenus sont réutilisés par les géants du numérique.

[15] Le Monde avec AFP, « Le "New York Times" poursuit en justice Microsoft et OpenAI, créateur de ChatGPT, pour violation de droits d'auteur », Le Monde, le 27 décembre 2023, [en ligne :] https://www.lemonde.fr/economie/article/2024/11/08/droits-voisins-une-cinquantaine-d-editeurs-de-presse-assignent-en-justice-microsoft_6383770_3234.html, consulté le 3 novembre 2024.

[16] Covolo J. avec Adam C., « A Liège, un des abris de nuit est accessible uniquement en ligne ou par téléphone : "Ça n'a pas de sens" », RTBF, le 22 octobre 2024, [en ligne :] https://www.rtbf.be/article/a-liege-un-des-abris-de-nuit-est-accessible-uniquement-en-ligne-ou-par-telephone-ca-n-a-pas-de-sens-11453040, consulté le 25 novembre 2024.

[17] La rédaction de l'ARC, « Numérique : qui paie la f(r)acture ? », ARC, novembre 2024, [en ligne :] https://www.arc-culture.be/numerique-qui-paie-la-facture/, consulté le 24 novembre 2024.

[18] L'ARC est un mouvement d'éducation permanente actif en Région bruxelloise et en Wallonie qui lutte pour le droit au respect, à la reconnaissance et au développement des pluralités culturelles qui composent notre société, qui soutient la capacité de chacun et chacune à faire valoir ce droit et qui vise l'émancipation de tous·tes.

[19] Nabat Y. et Verdon E., « La généralisation de la vidéosurveillance algorithmique fait peser des risques majeurs sur nos libertés », Le Monde, le 19 octobre 2024, [en ligne :] https://www.lemonde.fr/idees/article/2024/10/19/la-generalisation-de-la-videosurveillance-algorithmique-fait-peser-des-risques-majeurs-sur-nos-libertes_6355859_3232.html, consulté le 20 octobre 2024.

[20] La rédaction du Nouvel Obs, « Expérimentée pendant les Jeux de Paris, la vidéosurveillance algorithmique pourrait être généralisée », le Nouvel Obs, le 2 octobre 2024, [en ligne :] https://www.nouvelobs.com/societe/20241002.OBS94445/experimentee-pendant-les-jeux-de-paris-la-videosurveillance-algorithmique-pourrait-etre-generalisee.html, consulté le 15 octobre 2024.

[21] Lay A., Poulain B., Reynier M., Noel E., « Sécurité : la vidéo-surveillance plébiscitée par les communes, mais pas toujours efficace », Franceinfo, le 10 novembre 2022, , [en ligne :] https://www.francetvinfo.fr/replay-jt/france-3/19-20/securite-la-video-surveillance-plebiscitee-par-les-communes-mais-pas-toujours-efficace_5469783.html, consulté le 20 octobre 2024.

[22] Entretien avec Mhalla A., « Les Big Tech œuvrent à une privatisation du futur », Philonomist, le 28 février 2024, [en ligne :] https://www.philonomist.com/fr/entretien/les-big-tech-oeuvrent-une-privatisation-du-futur, consulté le 12 novembre 2024.

[23] Younan S., « Européennes 2024 : quels sont les lobbies les plus puissants au Parlement européen ? », Capital, le 16mai 2024, [en ligne :] https://www.capital.fr/economie-politique/europeennes-2024-quels-sont-les-lobbies-les-plus-puissants-au-parlement-europeen-1496757, consulté le 15 octobre 2024.

[24] Ronsin S., « Pourquoi un utilisateur averti en vaut deux » dans « Le guide de l'intelligence artificielle », Le Point, Février-mars 2024. Bouquet J., « Face à la puissance des lobbys des GAFAM, l'Union européenne fait-elle le poids ? », Rtbf.be, 15 décembre 2020, [en ligne :] https://www.rtbf.be/article/face-a-la-puissance-des-lobbys-des-gafam-lunion-europeenne-fait-elle-le-poids-10654184, consulté le 1er juin 2023.

Illustrations :
Citoyenneté & Participation, d'après Dooder (Freepik.com)

Citoyenneté & Participation (CPCP ASBL)
Avenue des Arts, 50 – 1000 Bruxelles
www.cpcp.be | 02 318 44 33 | info@cpcp.be

RPM Bruxelles - BCE : 0409.117.690 - IBAN : BE67 3101 6586 0487