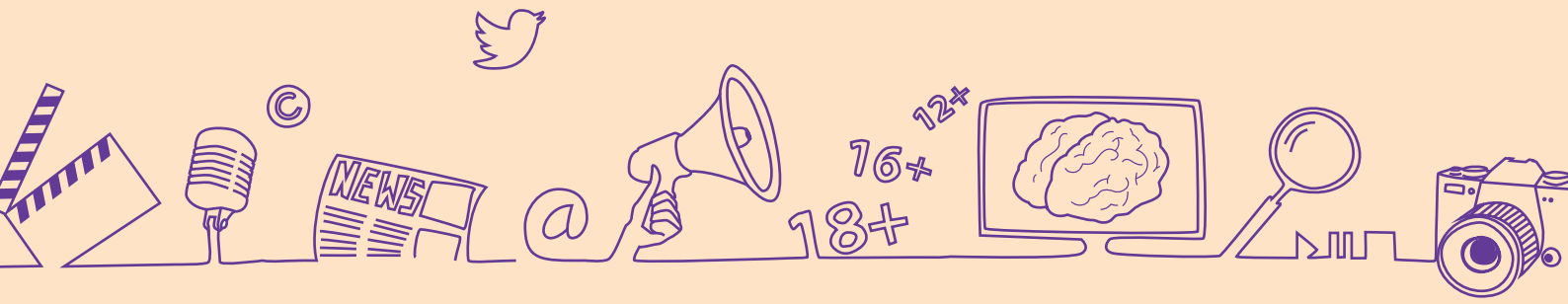
2024 | Étude | # 48

Médias & Actions citoyennes | Philippe Courteille

Les dangers démocratiques du numérique



Citoyenneté & Participation

: lien consultable ou téléchargeable

TABLE DES MATIÈRES

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.

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.

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.

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 (divisé) 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.

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.

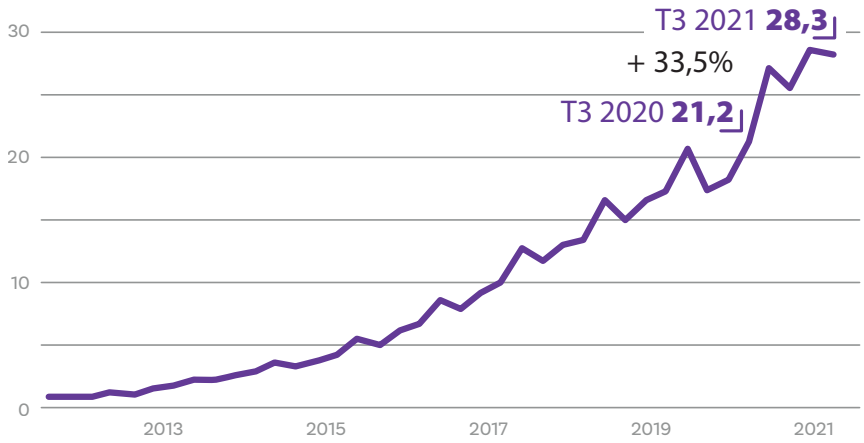
I. QUAND LES GAFAM, BATX ET AUTRES NATU, IMPOSENT LEUR FONCTIONNEMENT

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

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

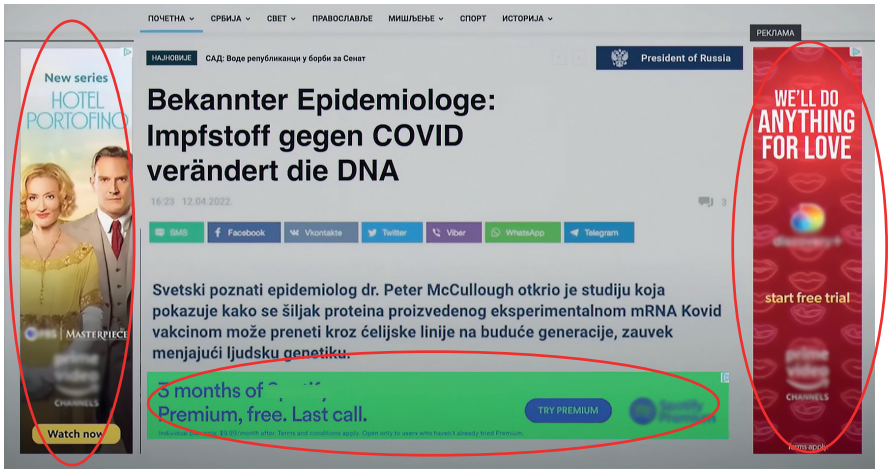
6 Diffusé dans l'émission Doc Shot sur la Une, *RTBF*, le 13 juin 2024 à 22h35.

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.

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.

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.

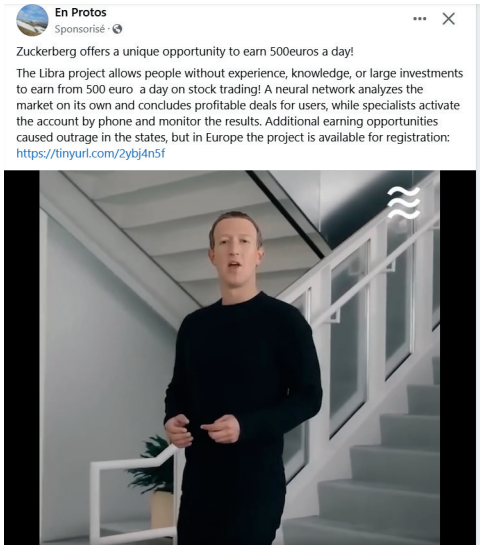
L'annonce est alléchante et Jammi Nandini rêve déjà de voir sa publicité diffusée sur des sites comme CNN ou le *Washington Post*. Quelle ne fut pas sa stupéfaction de découvrir la publicité sur le site de Breitbar, un journal de l'alt-right[8] américaine, considéré comme suprémaciste et complotiste. 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

8 L'extrême droite américaine.

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 ?



Zuckerberg offre une opportunité unique de gagner 500 euros par jour ! Le projet Libra permet aux personnes sans expérience, sans connaissances ou sans investissements importants de gagner à partir de 500 euros par jour en bourse. Un réseau de neurones analyse lui-même le marché et conclut des offres rentables pour les utilisateurs, tandis que des spécialistes activent le compte par téléphone et surveillent les résultats. Des opportunités de revenus supplémentaires ont provoqué l'indignation aux États-Unis, mais en Europe, le projet est disponible à l'enregistrement

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 algorithmes 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].

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.

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.

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.

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.

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.

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*

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.

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.

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 capt*ent 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

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.

« *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 importante 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

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.

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.

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.

II. 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 ou de vos recherches en ligne, de vos lies

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 du cahier sur le numérique 2024, de Citoyenneté & Participation ; 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.

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.

« 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, l eurs 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 person-

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.

nelles, 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, 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 :

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.

- 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 cents 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].

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.

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.

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*

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.

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.

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, shǒ uxìn). Mais le système est également un instrument politique, destiné à étouffer les critiques du régime.

III. 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.

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 plu-

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.

sieurs 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.

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.

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].

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 de 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

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.

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

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.

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].

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

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.

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 délirant 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 ins-*

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.

crits 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].

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

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.

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.

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.

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" … Le DSA, le Digital Services Act,*

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.

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 Electoral : 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 « i*nstrumentalisation 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*

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

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 Mais PB : « *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.

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 (ancien-

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 0 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.

nement 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].

IV. 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.

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.

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 ?

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, fonc-

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.

tions 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 ?* » …

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.

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 man-

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.*

quait 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.

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 ».

V. 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.

REPUBLIQUE FRANÇAISE
Liberté – Egalité – 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 – PEDOPHILIE – 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, spécialisée 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 chaines 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 : olivierzoudard10@gmail.com / olivierzoudard10@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

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 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.

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.

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 quatre cent septante-cinq mille 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 mille quatre cent septante-deux lits agréés, emploie plus de trois mille sept cents 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

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.

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*

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.

acteurs étatiques, en particulier ceux de la Russie et de la Chine. En fait, 92 % de la désinformation 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'abris 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*

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.*

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'ultradroite. 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*

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.*

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.

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 Emirats arabes unis, au Kazakhstan, en l'Azerbaïdjan,

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.

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 ?

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.

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 ?

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-XCKV6NXYGJGW7H3FTIOQ-2CASPQ, 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-JGWJXHFPXNCTDBMEDORQ5QYGN4, 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.

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.

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*

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.

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 telecom 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

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.

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 33000 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 … cinquante mille sept cents 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

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.*

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 !

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

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.

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,

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 Etats-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.

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'Etat à qui l'on confie, sans marchés publics transparents, les bases de données centralisées ou les algorithmes de traitement de nos données* » [161] .

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

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.

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

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.

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 règlementations 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 NYTimes 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.

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.

VI. 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. 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.

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.

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

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.

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,

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

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 ?

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.

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].

**

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.

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

COURTEILLE Philippe, *Les dangers démocratiques du numérique*, Bruxelles : Citoyenneté & Participation, Étude n°48, 2024, [en ligne :] http://www.cpcp.be/publications/e48-danger-demo-numerique.

Désireux d'en savoir plus !

Animation, conférence, table ronde... n'hésitez pas à nous contacter,
Nous sommes à votre service pour organiser des activités sur cette thématique.

www.cpcp.be

FÉDÉRATION
WALLONIE-BRUXELLES

Avec le soutien du Ministère de la Fédération Wallonie-Bruxelles

CPCP ASBL – Avenue des Arts 50/bte 6 – 1000 Bruxelles | info@cpcp.be | www.cpcp.be
N° d'entreprise : 0409 117 690 | RPM Bruxelles | BE67 3101 6586 0487

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 ou NATU, 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.

Citoyenneté & Participation

Avenue des Arts, 50/6 – 1000 Bruxelles
02 318 44 33 | info@cpcp.be
www.cpcp.be | www.facebook.com/CPCPasbl

Toutes nos publications sont disponibles en téléchargement libre :
www.cpcp.be/publications/

E.R. : John Lewis – Avenue des Arts; 50/6 – 1000 Bruxelles