LA GRANDE DÉPOSSESSION

Fondation Jean Jaurès

LA GRANDE DÉPOSSESSION
POUR UNE ÉTHIQUE NUMÉRIQUE EUROPÉENNE

MAXIME DES GAYETS

FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES
FONDATION EUROPÉENNE D'ÉTUDES PROGRESSISTES

Fondation Jean Jaurès

LA GRANDE DÉPOSSESSION
POUR UNE ÉTHIQUE NUMÉRIQUE EUROPÉENNE

MAXIME DES GAYETS

Maxime des Gayets, consultant en cybersécurité et résilience des entreprises, est conseiller régional d'Île-de-France.

Photographie de couverture : © Sebestyen Balint / Shutterstock

INTRODUCTION

La numérisation est la religion de ce nouveau siècle. D'un pas accéléré, la conversion de l'économie mondiale aux nouvelles potentialités du numérique et du développement d'Internet n'en finit plus de bousculer nos sociétés. En cinq ans, la quantité de données produites et échangées dans le monde a été multipliée par sept[1]. En France, l'économie numérique représente déjà plus du quart du PIB[2]. Et dans le tourbillon des 269 milliards de courriels quotidiennement envoyés[3], chacun se trouve affecté par cette extension continue du progrès technologique. Demain, ce ne sont plus seulement les femmes et les hommes, mais les objets qui seront reliés par la technologie : 15 % seront connectés d'ici à 2020, générant un chiffre d'affaires de près de 3 000 milliards d'euros[4].

Comment ne pas vouloir participer à ces mouvements qui offrent autant de potentialités que de transformations, qui refondent le temps comme les distances, qui modifient les chaînes de valeur autant que les modes de gouvernance ? Toutes les entreprises se convertissent à l'économie des données, les gouvernements investissent avec raison dans ce qui fait figure de nouvelle économie. Mais, l'humain ne s'effaçant pas dans cette marche, c'est aussi avec le souffle court que

1. « Big Data : 90 % des données existantes ont été créées ces deux dernières années », Comarketing news, 15 mars 2016.
2. Bruno Berthon (directeur général d'Accenture Strategy et responsable mondial de la stratégie digitale), « 3 idées reçues sur l'économie numérique », tribune publiée dans *Les Échos*, 12 avril 2016.
3. Radicati Group, *Email Statistics Report, 2017-2021*, Palo Alto, février 2017.
4. Communiqué de presse de l'agence de conseil Gartner, février 2017.

nos sociétés subissent les conséquences de ces transformations. L'absence de maîtrise fait naître l'angoisse.

Il en est ainsi s'agissant de la collecte massive des données sur Internet, qui recèle sa part de promesses et de démons. Du recueil au traitement, des algorithmes aux pratiques, se mêlent tout à la fois les possibilités de progrès et les risques d'excès. Le recours au big data permet déjà à une entreprise d'améliorer sa capacité à prendre une bonne décision grâce à l'analyse des données. Dans le secteur de la mobilité comme de la santé, l'usage de jeux de données massifs produit des services inédits par le jeu des modélisations. Mais des voix s'élèvent pour rappeler que ces informations sont autant d'instruments permettant la prédictibilité, le contrôle – et, d'une certaine manière, la dépossession – de ce que l'on est comme de ce que l'on fait.

Ces données peuvent opérer des transferts de valeur qui inversent les principes mêmes de nos économies. Jusqu'à l'excès ? Fondée en 2011, la société américaine MoviePass a lancé un forfait de cinéma permettant de voir un film par jour pour moins de 10 dollars par mois[1], soit pratiquement le prix d'une place de cinéma. La rentabilisation de cette offre s'appuie sur la récolte de données que l'entreprise pourra revendre. Comme si, dorénavant, ce n'était pas la consommation d'un bien, mais l'information sur son usage qui contenait de la valeur. Renversant.

Tout va vite, très vite. Et cela exacerbe les contradictions. Ainsi, la productivité permise par le déploiement des courriels dans les entreprises est contrecarrée par les mésusages. Un cadre passe cinq heures par jour à consulter ses messages, et lorsqu'il est interrompu par la réception d'un courriel, il lui faut plus d'une minute pour se

1. Liam Stack, « MoviePass Drops Its Price, Pleasing Customers but Angering AMC », *New York Times*, 25 août 2017.

concentrer à nouveau sur sa tâche[1]. Par le jeu de la communication virtuelle plutôt que réelle, les chaînes de décision se retrouvent fractionnées par des remises en cause permanentes. Comme le relève Dominique Wolton, « l'information accessible est devenue une tyrannie. Il y en a trop, accessible trop rapidement[2] », ce qui a pour conséquence de casser les hiérarchies des priorités.

Tel le ressac, ce sont aussi des vagues régulières de révélations qui viennent désormais briser la confiance envers la nouvelle donne technologique. Piratage industriel, cyberattaques provoquant le black-out de centaines d'entreprises, divulgation des données personnelles de milliers de clients, publication des correspondances de dirigeants… Plus une semaine ne passe sans que l'opinion publique ne soit interpellée par les faiblesses de nos systèmes informatiques. Selon l'étude de Dell EMC *Global Index Data Protection 2016*[3], une entreprise sur trois aurait perdu des données confidentielles à la suite d'une violation de sécurité. Face à ces nouvelles incertitudes, le niveau de protection de leurs données personnelles inquiète neuf Français sur dix[4]. Et de multiples fragilités commencent à scintiller dans le brouillard de la révolution numérique.

Il faut dire que la situation actuelle concentre tous les ingrédients d'un grand désordre. Une des raisons à cela est la suprématie d'acteurs économiques qui, en quelques années, ont bouleversé les rapports de pouvoir dans la mondialisation. Les entreprises du numérique ont constitué des empires que les pouvoirs publics peinent à encadrer.

1. Tomas W. Jackson, Ray Dawson et Darren Wilson, « Understanding email interaction increases organizational productivity », *Communications of the ACM*, vol. 46, n° 8, 2003, pp. 80-84 ; Laura Marulanda-Carter et Thomas W. Jackson, « Effects of e-mail addiction and interruptions on employees », *Journal of Systems and Information Technology*, vol. 14, 2012, pp. 82-94.
2. Cité *in* « L'"infobésité", un nouveau fléau dans l'entreprise », *L'Obs*, 31 août 2012.
3. Dell EMC, *Global Index Data Protection 2016*, juin 2016.
4. CSA, *Les Français et la protection de leurs données personnelles*, 19 septembre 2017.

Cumulant des positions quasi monopolistiques et une capacité continue de digestion de nouvelles fonctionnalités, ces ogres contemporains se déploient avec voracité dans les moindres recoins de nos sociétés. Devant la féerie technologique qui alimente tous les rêves, la lucidité manque pour percevoir que les menaces escamotent les promesses. Une autre raison est l'immixtion de la révolution numérique dans le quotidien de chacun. L'hyperconnexion envahit l'espace privé et le restreint. Par manque d'apprentissage, les utilisateurs des nouvelles technologies se perdent dans un tumulte de contradictions et de mésusages. Provoquant autant de confusions que de nouvelles formes de contrôle social, affaiblissant le libre arbitre et écornant l'idée même de souveraineté numérique.

Doit-on dès lors tourner le dos à ce bouleversement qui puise sa puissance dans le progrès technologique ? Ce serait oublier que chaque révolution s'accomplit dans un mouvement chaotique et discontinu où la soif de transformation doit céder le pas à l'urgence de sa domestication. Nous nous trouvons à la croisée des chemins, dans ce clair-obscur qui favorise les excès et les insuffisances, où s'engouffrent les malveillants et ceux qui veulent agir pour leur seul profit. Pour faire preuve de maîtrise, il faut donc de la clairvoyance. Même de plus en plus fréquents, les soubresauts liés aux révélations sur l'usage par les réseaux sociaux de nos données personnelles ne peuvent suffire à nous faire ouvrir les yeux sur l'ampleur des enjeux existants. Un débat en profondeur doit émerger. Le présent ouvrage se veut une contribution à cette prise de conscience nécessaire.

Demain, le couple homme-machine accouchera d'un monstre s'il n'est pas encadré par une éthique qui lui donne un sens et des repères. Or, celle-ci ne peut émerger facilement lorsque les besoins sociaux se confondent avec des besoins individuels, que les avantages octroyés masquent les contreparties exigées, que la puissance des technologies

réfute leurs fragilités inhérentes. Ces confusions renforcent ce que Herbert Marcuse considérait déjà à son époque comme l'un des plus fâcheux aspects de la société industrielle avancée : le caractère rationnel de son irrationalité[1]. Nous ne pourrons retrouver raison en restant silencieux sur la destination que nous nous fixons sur le chemin de la modernité. Savoir où l'on va et pouvoir en discuter, n'est-ce pas la première des souverainetés ?

1. Herbert Marcuse, *L'Homme unidimensionnel. Études sur l'idéologie de la société industrielle*, Paris, Minuit, 1968.

L'EFFET DE BASCULE

Si la révolution numérique touche quotidiennement chacun de nous, elle a également transformé le visage de nos économies.

DE NOUVEAUX OGRES

Pour prendre conscience du changement, il suffit de s'attarder quelques instants sur l'évolution de la hiérarchie mondiale des grands groupes. En l'espace d'une grosse décennie, les entreprises du numérique se sont hissées au premier rang des capitalisations boursières. Apple, Google (Alphabet Inc.) et Microsoft se partagent un podium qui, dans les années 1980, était accaparé par les industries pétrolières, automobiles ou chimiques.

En 1997, le Financial Times Global 500, ce classement mondial des sociétés par capitalisation boursière[1], fait apparaître par ordre décroissant les entreprises suivantes : General Electric (États-Unis), Royal Dutch Shell (Pays-Bas), Microsoft (États-Unis), ExxonMobil (États-Unis), The Coca-Cola Company (États-Unis), Intel Corporation (États-Unis), Nippon Telegraph and Telephone (Japon), Merck (États-Unis), Toyota Motor Corporation (Japon), Novartis (Suisse).

1. Publié chaque année par le *Financial Times*, il est disponible sur le site www.ft.com/ft500

Vingt ans plus tard, ce classement a été profondément bouleversé par l'émergence de la « nouvelle économie ». En juin 2017, la hiérarchie des plus grandes capitalisations boursières est la suivante : Apple, Alphabet Inc., Microsoft, Amazon.com, Berkshire Hathaway, Facebook, ExxonMobil, Johnson & Johnson, JPMorgan Chase & Co. et Wells Fargo & Co[1]. Sur ces dix entreprises – toutes américaines –, la moitié appartiennent au secteur des nouvelles technologies.

Cette domination financière se distingue de ce que nous avions connu jusqu'à présent dans l'économie mondiale, par son ampleur, ses caractéristiques et ses effets de concentration. Tout d'abord, les GAFAM[2] disposent de moyens inégalés pour assécher les dynamiques de concurrence du marché. Google a ainsi multiplié les rachats d'entreprises dans le domaine des nouvelles technologies, tout comme les autres géants du numérique, qui ont mis la main sur des centaines de start-up en vue d'acquérir leur expertise et leur technologie. Ces dernières années, ces ogres du numérique ont ainsi dévoré un tiers des fusions-acquisitions du secteur et pu déposer en moins de dix ans plus de 52 000 brevets dans le domaine de l'intelligence artificielle[3]. Ensuite, par leur situation de quasi-monopole, ces acteurs disposent d'une rente de situation qui leur permet de s'imposer facilement dans d'autres secteurs économiques. Quand on sait que 90 % de l'activité des moteurs de recherche dans le monde sont assurés par Google ou que 75 % des pages vues sur les réseaux sociaux aux États-Unis concernent Facebook, on comprend mieux pourquoi ces deux entreprises ont raflé 20 % des investissements publicitaires mondiaux en 2017[4]… Selon l'étude

1. PricewaterhouseCoopers (PwC), « Global Top 100 Companies by market capitalisation », 28 juin 2017.
2. Les actuels géants du Web sont surnommés GAFA ou GAFAM, acronyme constitué des firmes les plus puissantes (Google, Apple, Facebook, Amazon, Microsoft).
3. « The Race For AI: Google, Intel, Apple In A Rush To Grab Artificial Intelligence Startups », CB Insights, 27 février 2018.
4. Zenith Media, « Top Thirty Global Media Owners », 9 juin 2017.

annuelle de l'Observatoire de l'e-publicité, 78 % du marché français sont ainsi captés par Facebook et Google[1]. Enfin, cette puissance des GAFAM se caractérise par sa structure peu pourvoyeuse d'emplois. Si ces entreprises ont une capitalisation boursière désormais équivalente au PIB de l'Allemagne[2], elles comptent relativement peu de salariés à travers le monde. Le cumul des effectifs de Google, Facebook, Apple et Amazon ne représente qu'un peu plus de 500 000 personnes[3]. Amazon n'est que le 74e employeur des États-Unis, Apple ne figurant pas dans les deux cents premiers[4]…

Ces géants ne semblent avoir ni limites, ni frontières, et prétendent exercer leur souveraineté au nom de leur puissance. Comment ne pas voir cette ambition dans les arguments avancés par Apple pour contester le redressement record de 13 milliards d'euros infligé par la Commission européenne à l'été 2016 au titre de l'impôt des sociétés[5] ? La société américaine considère qu'elle ne peut être soumise à un régime fiscal commun. Sa puissance justifierait qu'elle puisse choisir sa territorialité fiscale et les modalités de son imposition. C'est ce qu'elle a fait avec l'Irlande qui, pour la marque à la pomme, a accepté de baisser son taux d'imposition des bénéfices – déjà le plus bas d'Europe – de 12,5 % à… 1 %[6].

1. 19e Observatoire de l'e-pub SRI, réalisé par le cabinet d'audit et de conseil PwC, en partenariat avec l'UDECAM, janvier 2018.
2. « La puissance économique des cinq géants du net a encore crû en 2017 », RTS Info, 3 février 2018.
3. Alexandre Mirlicourtois (directeur de la conjoncture et de la prévision chez Xerfi), « L'envol des géants du numérique... pauvres en emplois », tribune publiée dans *La Tribune*, 19 avril 2017.
4. Christophe Bys, « À eux 5, les Gafa+Microsoft représentent autant d'emplois que Carrefour », *L'Usine digitale*, 13 avril 2017.
5. Commission européenne, « Aides d'État : l'Irlande a accordé pour 13 milliards d'EUR d'avantages fiscaux illégaux à Apple », communiqué de presse, Bruxelles, 30 août 2016 ; Commission européenne, « Aides d'État : la Commission assigne l'Irlande devant la Cour de justice pour non-récupération des 13 milliards d'euros d'avantages fiscaux perçus illégalement par Apple », communiqué de presse, Bruxelles, 4 octobre 2017.
6. *Ibid.* ; « L'Irlande va collecter auprès d'Apple les arriérés d'impôt exigés par Bruxelles », *Le Monde*, 5 décembre 2017.

Si les institutions européennes se sont récemment réveillées pour mettre fin à ce régime d'exception[1], le poids économique des GAFAM rend bien difficile un retournement du rapport de force. Certains préfèrent d'ailleurs reconnaître cet état de fait et en tirer les conséquences les plus inédites. Il en est ainsi du ministre des Affaires étrangères danois, Anders Samuelsen. Au début de l'année 2017, il a annoncé la nomination d'un ambassadeur auprès des GAFAM. Pour le Danemark, « les temps nouveaux requièrent de nouvelles approches diplomatiques[2] »… au risque d'élever ces firmes au rang de puissances diplomatiques, et donc de quasi-États.

Dans ce monde hyperconnecté, il semble bien difficile pour les États-nations de réussir à imposer des règles de régulation à des acteurs dont le terrain de jeu est aussi déterritorialisé. Certains pourraient s'en féliciter en évoquant les chances offertes par une mondialisation des réseaux sociaux qui défie les régimes les plus autoritaires en débridant les capacités d'opinion, d'expression et d'information des citoyens. Mais ce serait taire les barrières qui ont été édifiées dans certains pays pour limiter l'accès à Internet. Facebook et Twitter sont inaccessibles en Chine depuis 2009. Cette absence a été « compensée » dans les usages par le déploiement du réseau social WeChat qui, selon le patron de cette entreprise, aurait dépassé le milliard d'utilisateurs en mars 2018[3]. Mais, si le pays laisse l'usage de cet outil d'échange se développer dans la population, les autorités se sont donné les moyens d'en contrôler

1. Le 21 mars 2018, la Commission européenne a proposé de nouvelles règles afin que les activités des entreprises numériques soient imposées d'une manière équitable et propice à la croissance : Commission européenne, « Imposition de l'économie numérique : la Commission propose de nouvelles mesures pour garantir que toutes les entreprises paient leur juste part d'impôt dans l'UE », communiqué de presse, Bruxelles, 21 mars 2018.
2. Tweet des autorités danoises cité par Alexis Feertchak, « Le Danemark aura un ambassadeur dans la Silicon Valley », *Le Figaro*, 1er février 2017.
3. « L'application chinoise WeChat dépasse le milliard d'utilisateurs », *Les Échos*, 6 mars 2018.

fortement le contenu. C'est ce qu'ont démontré les chercheurs du Citizen Lab de Toronto dans une série d'études publiées en 2016[1]. Selon les mots utilisés ou les thèmes retenus, les messages diffusés sur ce réseau social peuvent instantanément disparaître sans jamais atteindre leur destinataire. Ces nouvelles formes de censure représentent un marché florissant où prospèrent des entreprises américaines ou canadiennes, rivalisant d'imagination pour mieux bloquer celle des utilisateurs… Les outils Websense, SmartFilter ou encore Netsweeper ont ainsi assuré le filtrage d'Internet dans plusieurs pays du Golfe[2] sans rencontrer de réprobation de leur propre gouvernement. Même l'entreprise Apple n'a pas hésité à passer un accord avec les autorités de Pékin le 28 février 2018[3] pour leur permettre l'accès aux données iCloud des utilisateurs chinois, rognant ainsi sur ses propres règles de protection des informations de ses clients.

DE NOUVEAUX RISQUES

Pourtant, même si elles sont connues, ces capacités du numérique à filtrer les informations ou, au contraire, à en multiplier les exploitations, ne suffisent pas encore à ébranler la confiance de chacun dans l'usage des nouvelles technologies et à permettre de mesurer clairement l'ampleur des menaces. C'est en effet la compréhension même de ce qui est en jeu qui n'est ni partagée, ni assumée par les acteurs. Un

1. Lotus Ruan, Jeffrey Knockel, Jason Q. Ng et Masashi Crete-Nishihata, *One App, Two Systems. How WeChat uses one censorship policy in China and another internationally*, The Citizen Lab, 30 novembre 2016.
2. Helmi Noman et Jillian C. York, *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011*, OpenNet Initiative, mars 2011.
3. Élisa Braun, « Données : Apple se plie aux exigences de la Chine », *Le Figaro*, 26 février 2018.

producteur de céréales accepterait-il de voir ses sacs de blé éventrés au point de perdre régulièrement une partie de sa récolte ? C'est la même mécanique qui est à l'œuvre aujourd'hui dans l'ère du numérique, lorsque les données d'une organisation s'éparpillent sur le Web. Selon le rapport *Breach Level Index* 2017 publié par la société Gemalto, c'est près de 2,5 milliards de données qui ont été volées au cours de cette année-là dans le monde, provenant essentiellement de sites web ou de serveurs d'entreprises, soit une augmentation de 88 % par rapport à l'année 2016[1].

Cette situation résulte d'une double inconscience persistante : non seulement on sous-estime les risques relatifs à l'usage des outils digitaux, mais on ne mesure pas davantage la valeur des données qui circulent dans notre société moderne. À cet égard, la controverse concernant les courriels de Hillary Clinton en mars 2015 offre un exemple éclairant. La candidate démocrate a été mise en cause pour avoir utilisé une messagerie non sécurisée lorsqu'elle était secrétaire d'État. Cette affaire a puissamment ébranlé sa campagne et offert un angle d'attaque majeur au camp républicain. C'est par une double négligence, en ne mesurant pas les risques de fuite, mais également la valeur des informations transmises (et l'usage qui pouvait en être fait) que Hillary Clinton s'est exposée en utilisant une messagerie privée pour l'envoi de ses courriels.

Alors qu'une secrétaire d'État peut agir ainsi, comment espérer de chaque individu ou entité une attitude préventive s'ils n'ont pas la pleine conscience des risques, mais aussi de la valeur de ce qu'ils échangent ? Cette inconscience, associée à la complexité d'usage des outils sécurisés, explique que 80 % des salariés utilisent des solutions informatiques sans l'accord formel de leur directeur des systèmes

1. Michelle Leech, « 2017 Data Breach Level Index: Full year results are in… », Gemalto, 13 avril 2018.

d'information (DSI)[1]. Ce phénomène, appelé « Shadow IT », n'est évidemment pas étranger au fait que 63 % des incidents de sécurité proviennent directement du comportement d'un salarié malintentionné, ou simplement d'une erreur de sa part[2].

Le nécessaire renforcement des outils de cybersécurité ne pourra seul répondre aux stratégies de contournement des usagers. Face au risque que représentent les nombreux détenteurs de clés USB qui les utilisent pour des transferts entre le travail et le domicile, le meilleur réseau informatique restera inopérant… En témoigne la découverte étonnante par un passant d'une clé USB sur un trottoir londonien en octobre 2017. Non cryptée, celle-ci contenait 76 dossiers confidentiels (cartes, vidéos, documents) liés à la sécurité de l'aéroport d'Heathrow, dont les horaires des patrouilles de police, le positionnement des caméras de surveillance ou les itinéraires de la reine Elizabeth II[3]… Au-delà des systèmes et des infrastructures, ce sont donc les pratiques individuelles qui doivent être encadrées. La sécurité des systèmes informatiques n'est plus seulement une question technique dont la responsabilité reposerait uniquement sur le directeur des systèmes d'information. C'est désormais un enjeu global qui traverse toute l'entreprise car il dépend du comportement de tous les salariés. Dans de nombreuses entreprises, sous l'impulsion des évolutions de la réglementation européenne, ce mouvement est engagé, plaçant la sécurité des réseaux d'information au niveau de la direction exécutive. Mais une prise de conscience efficiente des enjeux posés par la

1. *The Hidden Truth Behind Shadow IT. Six trends impacting your security posture*, Stratecast et Frost & Sullivan, novembre 2013. Ces pratiques ont aussi fait l'objet d'une étude plus récente du groupe NTT Communications Corporation confirmant la même tendance : *The People versus the Ministry of No* (8 juin 2016).
2. Étude du cabinet Deloitte, « Les grandes tendances dans la cybersécurité », 18 janvier 2018.
3. Dan Warburton, « Terror threat as Heathrow Airport security files found dumped in the street », *Mirror*, 28 octobre 2017.

révolution numérique nécessite aussi de faire comprendre à chaque salarié en quoi ce qu'il produit, ce qu'il échange et ce qu'il manipule constitue le capital vital de l'organisation.

L'ère numérique et l'une de ses conséquences, le décloisonnement managérial, font de chaque acteur le détenteur d'une des clés d'accès à la valeur ajoutée produite. Il est commun de dire que la lecture de quelques semaines de correspondance interne d'une entreprise suffit pour récupérer une grande partie de sa production intellectuelle. Car par la numérisation, la valeur ajoutée se trouve bien souvent diffuse… et diffusée. Cette richesse n'est pas toujours correctement appréhendée, et donc protégée.

Pourtant, il est fréquent qu'un salarié amené à quitter son entreprise décide – par réflexe ou intérêt – de conserver des données confidentielles appartenant à son employeur. Selon une étude de la société Symantec menée en 2013, une personne sur deux a agi de la sorte après une démission ou un licenciement[1] avec souvent l'idée de se réserver la possibilité d'utiliser ces données dans son nouvel emploi. Ces attitudes ne sont certes pas nouvelles. Avant l'ère numérique, des employés pouvaient déjà emporter avec eux leur « fichier clients ». Mais la méconnaissance des enjeux, la miniaturisation des espaces de stockage, les usages du numérique ont donné une autre dimension à ces pratiques. Avec ces transformations, c'est une responsabilité considérable qui est confiée à chacun. Les dirigeants doivent la reconnaître pour qu'elle puisse être acceptée et exercée par les salariés. Or, l'information et la donnée produites sont encore puissamment sous-estimées, n'étant vécues que comme des richesses à exploiter en soi alors qu'elles sont devenues indispensables à toute activité. Cette

1. Guido Sanchidrian, « What's yours in mine? How employees are putting your intellectual property at risk », enquête Symantec, février 2013.

dépendance bouleverse la solidité des acteurs, qui sont confrontés aux vulnérabilités de leurs infra-structures informatiques face à la multiplication des cyberattaques.

Selon une importante firme spécialisée dans la récupération de données, Kroll Ontrack, 60 % des entreprises ayant perdu leurs données seraient contraintes de fermer leurs portes dans les six mois qui suivent[1]. D'après l'étude mondiale menée par IBM et Ponemon Institute, le coût moyen d'une violation de données s'établissait en 2017 à 3,62 millions de dollars[2]. Si la fuite des données représente un coût majeur pour l'entreprise, cette dernière doit pouvoir y accéder pour que ses activités n'en pâtissent pas. En juin 2017, ce sont plusieurs géants de l'économie – dont le groupe français Saint-Gobain et le numéro un du transport maritime Maersk – qui se sont retrouvés en situation de black-out à la suite du déploiement de deux virus bloquant l'accès à leurs services informatiques.

Ces exemples permettent de comprendre que, dans la révolution numérique, le capital ne se situe plus seulement dans la propriété des moyens de production, mais aussi dans leur protection. Cette transformation doit modifier le rapport entre l'entreprise et ses salariés puisque ceux-ci sont devenus pleinement dépositaires de la survie du capital. Pour le dire autrement, la sécurisation des pratiques numériques dans une entreprise ne peut être efficiente si elle reste cantonnée à une injonction du DSI. Elle doit s'appuyer sur une réévaluation de la responsabilité de chaque employé – et donc de sa reconnaissance – afin qu'il puisse adhérer à cette exigence. Il s'agit là d'un enjeu majeur de management des équipes au sein des entreprises.

1. Jérôme Dajoux, « La perte de données, une cause importante de faillite des entreprises », *Informanews*, 15 novembre 2017.
2. *2017 Cost of Data Breach Study*, Ponemon Institute LLC, juin 2017.

Celles-ci ne peuvent réduire les risques de fuite de données dans une logique uniquement descendante, qui ne favoriserait pas une vigilance active de l'ensemble des salariés.

DE NOUVELLES VULNÉRABILITÉS

Bouleversant de fait l'organisation du travail, les échanges digitaux occupent une place considérable dans le fonctionnement de nos sociétés. Au-delà même de l'usage frénétique des réseaux sociaux, la plus grande partie des interactions utilise des formats numériques. Le 1,4 milliard de courriels[1] échangé quotidiennement en France concerne l'activité des entreprises, la vie professionnelle comme la vie privée. La dématérialisation se déploie à grande vitesse, les recherches d'emploi, de transport ou même l'accès à la santé font l'objet d'applications performantes et populaires. Rien ne semble pouvoir arrêter ce basculement global vers le numérique, alors que ces échanges exposent à des vulnérabilités qui devraient en freiner les usages.

Ce que nous ne pourrions accepter dans le « réel » est toléré sur le Web. Dans une société démocratique, personne ne supporterait de constater que son courrier est décacheté avant qu'il n'en ait pris connaissance, que ses discussions sont épiées par un voisin caché derrière une porte ou que son appartement est fouillé régulièrement – et cambriolé. Ces tolérances aux vulnérabilités du numérique doivent beaucoup aux « effets de réseaux » dont Michael L. Katz et Carl Shapiro ont depuis longtemps cerné les différentes natures[2]. C'est le nombre

1. Radicati Group, *Email Statistics Report, 2016-2020*, mars 2016.
2. Michael L. Katz et Carl Shapiro, « Network Externalities, Competition, and Compatibility », *The American Economic Review*, vol. 75, n° 3, juin 1985, pp. 424-440.

d'utilisateurs qui fonde l'utilité des services de messagerie comme des réseaux sociaux. Cette externalité positive engendre non seulement des situations potentielles de monopole pour des technologies attractives, mais crée également un capital de confiance auprès des utilisateurs : plus les utilisateurs sont nombreux, plus on s'y fie. Pour paraphraser Georg Simmel[1], c'est l'ampleur d'un même usage qui détermine la certitude de ne pas être trompé. Ainsi, la confiance dans une technologie n'est pas tant jugée rationnellement que jaugée interactivement. Cette mécanique de confiance fondée sur un niveau d'usage constitue d'ailleurs le socle de développement des GAFAM, leur permettant d'ajouter des fonctionnalités à leurs outils sans que l'utilisateur se pose la question de sa dépossession.

À la fin de l'année 2017, une enquête du *New York Times* démontrait que plus de 250 applications de jeux mobiles intégraient un logiciel captant les sons émis à proximité de l'utilisateur, par un accès au micro du téléphone[2]. Ces données sonores pouvaient être collectées alors même que ni l'application concernée, ni même le téléphone n'étaient utilisés. Il s'agissait, via l'outil intégré Alphonso Automated Content Recognition (ACR), d'agréger des échantillons sonores pour déterminer les programmes télévisés suivis par les utilisateurs, à des fins de ciblage publicitaire.

C'est ainsi que, à partir de l'utilisation d'un simple jeu sur son mobile, comme Ping Pong Star, Black Jack ou Fishing 3D, on devient générateur d'informations, cible de publicités, client d'offres de transport, etc. Et c'est pourquoi, dans cette mécanique d'hyperconnexion, les impératifs de maîtrise et de sécurisation des données sont antinomiques avec le

1. André Tiran, « Confiance sociale, confiance primordiale en partant de Georg Simmel », *in* Philippe Bernoux et Jean-Michel Servet (dir.), *La Construction sociale de la confiance*, Paris, Montchrestien, 1997.
2. Sapna Maheshwari, « That Game on Your Phone May Be Tracking What You're Watching on TV », *New York Times*, 28 décembre 2017.

modèle même des GAFAM. Ceux-ci ne peuvent s'engager dans cette voie puisque c'est la dépossession même de la souveraineté numérique de leurs clients qui alimente leur croissance.

De plus, la satisfaction des utilisateurs dans l'accès à de nouveaux services contribue à minorer les vulnérabilités de sécurité. L'arbitrage entre les risques théoriques et les bénéfices réels ne remet pas en cause les usages, comme le démontre régulièrement le Baromètre de confiance des Français dans le numérique. Alors qu'ils ne sont que 37 % à avoir confiance dans le numérique, 83 % de nos concitoyens sont connectés à Internet. Et si 84 % ont pleinement conscience que leurs données personnelles sont utilisées par les réseaux sociaux, cela n'apparaît pas comme un frein à leur utilisation[1].

Comme nous l'avons souligné, ces paradoxes peuvent s'expliquer par l'incapacité à estimer la valeur des données que l'on produit ou diffuse. Pour beaucoup, celles-ci n'ont que peu de valeur et leur appropriation par autrui ou leur diffusion n'auraient pas de conséquences. Cette attitude est encouragée par le décalage qui peut exister entre le vol de données et leur usage malveillant. Contrairement aux idées reçues, l'utilisation immédiate des données récupérées frauduleusement sur le Web n'est pas toujours la règle. D'une part, la découverte du vol prend du temps[2]. Entre le lancement d'une attaque et sa découverte par les victimes, il s'écoule en moyenne près de six mois[3]. D'autre part, l'utilisation des données a souvent lieu plusieurs années après. On a ainsi d'autant plus de difficultés à prendre conscience des risques que leurs effets sont loin d'être immédiats. Les

1. 5e édition du Baromètre de confiance des Français dans le numérique, Harris Interactive, 21 octobre 2016.
2. Il a fallu ainsi attendre plus de dix ans pour découvrir qu'un groupe de hackers chinois espionnait plus de cent cinquante institutions et entreprises occidentales depuis le début des années 2000. Cela n'a été révélé qu'en 2014…
3. *M-trends 2018 report*, FireEye, 4 avril 2018.

dangers encourus ne sont donc perçus que très théoriquement par les citoyens comme par les entreprises.

Ainsi, les enquêtes menées à la suite de piratages d'ampleur soulignent souvent la négligence coupable des directions d'entreprise face aux risques. Le numéro trois de la grande distribution aux États-Unis, le groupe Target, a certes pu survivre au vol de données de ses clients à la fin de l'année 2013 (jusqu'à 110 millions de clients ont pu être concernés)[1]. Ce piratage informatique avait été estimé à plusieurs milliards de dollars[2], puis ramené à environ cent cinquante millions de dollars[3]. Mais le PDG, Gregg Steinhafel, a été dans l'obligation de démissionner quelques mois plus tard, pour couper court aux critiques sur le niveau de sécurité initial de son entreprise. Richard Smith, le patron de l'agence de crédit américaine Equifax, a connu le même sort à la suite d'une attaque informatique en septembre 2017 sur la base de données de 143 millions de ses clients[4]. Les pirates se seraient approprié les noms, les numéros de sécurité sociale et les numéros de permis de conduire de ses clients, permettant des usurpations d'identité à grande échelle. Et que dire de la société Uber qui n'a révélé qu'en novembre 2017 une fuite massive qui a eu lieu un an plus tôt, touchant 57 millions de ses clients et chauffeurs[5] ? On a fini par apprendre que la direction de l'entreprise n'avait pas hésité à payer le hacker pour qu'il taise son forfait[6]…

1. Elizabeth A. Harris et Nicole Perlroth, « For Target, the Breach Numbers Grow », *New York Times*, 10 janvier 2014.
2. Audrey Fournier, « Aux États-Unis, piratage géant des clients de Target », *Le Monde*, 22 mai 2104.
3. Rachel Abrams, « Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop », *New York Times*, 5 août 2014.
4. Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth et Ron Lieber, « Equifax Says Cyberattack May Have Affected 143 Million in the US », *New York Times*, 7 septembre 2017.
5. Julia Carrie Wong, « Uber concealed attack that exposed data of 57 million », Bloomberg news, 21 novembre 2017.
6. Nicole Periroth et Mike Isaac, « Inside Uber's $100,000 Payment to a Hacker, and the Fallout », *New York Times*, 12 janvier 2018.

Le jeune chercheur Charles Bazin faisait remarquer qu'aujourd'hui « Google connaît le moindre de vos déplacements grâce à Maps. Prism, révélé par Edward Snowden, serait capable d'écouter toutes les conversations du monde. » « La vie privée n'existe plus, mais est-ce si grave[1] ? » Nous répondrons que non, dès lors que chacun – qu'il soit individu, institution ou entreprise – garde sa souveraineté numérique, c'est-à-dire une maîtrise qui empêche toute dépossession. L'autonomie (d'autres parleront de résilience[2]) est évidemment indispensable, car la dépendance à des systèmes uniques constitue la principale fragilité des acteurs économiques comme des institutions. Le blocage des structures informatiques des entreprises est l'objectif des derniers virus. Alors que les solutions les plus populaires du marché s'appuient sur une logique d'intégration qui fait système, la survie de la société connectée passe au contraire par une pluralité de solutions existant de manière autonome et déconnectée du réseau informatique attaqué.

En effet, la mutualisation des données sur des supports uniques aboutit à une mutualisation préoccupante des vulnérabilités. C'est ainsi que la défaillance du seul service de *cloud computing* d'Amazon, au début de l'année 2017, a provoqué le dysfonctionnement de milliers de services qui en étaient clients. De Slack à Apple Store, de Dropbox au site de la Securities and Exchange Commission[3], c'est une partie importante du Web qui a été affectée durant plusieurs heures, en raison de l'absence de générateur de secours. Représentant plus d'un tiers du marché du

1. Charles Bazin, « Digitalisation, crise de confiance ou crise d'identité ? », *Génération Mobilité 8*, 31 mars 2017.
2. Florent Skrabacz, directeur général d'une entreprise de sécurisation des échanges, définit ainsi la résilience : « Acceptons une définition simplifiée […] : disposer de l'autonomie nécessaire pour reconstruire après un choc extrême », in « Résilience numérique : l'enjeu d'une Europe renouvelée », *SD Magazine*, 22 janvier 2018.
3. La Securities and Exchange Commission (SEC) est l'autorité américaine de réglementation et de contrôle des marchés financiers.

Cloud[1], hébergeant des données de 80 % des entreprises du CAC 40[2], le service cloud d'Amazon (AWS)[3] est devenu la première source de profit de l'entreprise américaine. Surtout, par cet effet de dépendance et le risque de déni de service (le fait que les services web ne soient plus disponibles), elle constitue l'une des fragilités les plus importantes de l'économie numérique.

Dans une note publiée par l'Institut français des relations internationales (Ifri), la chercheuse Gabrielle Desarnaud livre une analyse passionnante des vulnérabilités inhérentes à la conversion numérique de l'industrie énergétique et évoque les réponses qui y sont apportées. Mais elle insiste aussi sur les nouveaux risques en matière de cybersécurité : « Les réseaux intelligents et les compteurs communicants ont la particularité d'augmenter singulièrement le nombre de points d'entrée sur un réseau où s'échangent des données. Dans la mesure où les compteurs sont tous configurés de la même manière et peuvent donc être porteurs des mêmes failles, ils augmentent considérablement la surface d'attaque disponible. […] le développement de "l'Internet des objets" […] accentuera encore cette tendance. L'interaction d'appareils électriques privés dont l'usage ne peut être contrôlé (téléphone, portable, appareils électroménagers) avec des composantes du réseau électrique rendra les besoins en cybersécurité plus pressants encore[4]. » Alors que, d'après les prévisions, plus de 30 milliards d'objets connectés seront utilisés en 2021[5], les potentialités

1. « Cloud Market Keeps Growing at Over 40%; Amazon Still Increases its Share », *Synergy Research Group*, 27 octobre 2017.
2. Ridha Loukil, « 80 % des entreprises du CAC 40 utilisent le cloud d'Amazon selon Werner Vogels, CTO d'Amazon », *L'Usine digitale*, 25 juin 2015 ; Anaelle Grondin, «Une panne du cloud d'Amazon a impacté une centaine de milliers de sites web », *Les Échos*, 1er mars 2017.
3. « AWS Market Share Reaches Five-Year High Despite Microsoft Growth Surge », *Synergy Rechearch Group*, 2 février 2015.
4. Gabrielle Desarnaud, *Cyberattaques et systèmes énergétiques. Faire face au risque*, Paris, Ifri Centre Énergie, janvier 2017.
5. Chiffres de Verizon cités par le *Global Security Mag*, « Point de vue des tendances et évolutions du marché de l'IoT à l'horizon 2020 », décembre 2016.

de détournement sont vertigineuses et ont déjà été testées non seulement pour compromettre directement les utilisateurs, mais aussi pour démultiplier des attaques sur des tiers.

C'est ainsi par le déploiement du logiciel malveillant Mirai qu'il a été possible, en septembre 2016, de faire converger sur l'hébergeur OVH des requêtes de plus de 145 000 objets connectés piratés[1] pour tenter de le rendre indisponible. Cette attaque « botnet[2] » par déni de service s'est appuyée sur une armée de machines zombies (caméras de sécurité, routeurs installés dans des maisons, etc.) détournées de leur fonction. Elle a été possible parce que de nombreux fabricants répugnent à sécuriser leurs produits afin de réduire le coût de développement, d'assurer leur compatibilité et d'accélérer leur commercialisation[3]. Au-delà même de ces risques globaux, les objets connectés – par leur nature – ouvrent la voie à toute forme d'intrusion. Ces « portes ouvertes » sur les activités des utilisateurs ont été récemment à l'origine de tensions entre les services de renseignement américains et le leader chinois du marché du drone de loisir, l'entreprise DJI. En octobre 2017, une note du bureau de Los Angeles de l'Immigration and Customs Enforcement[4] expliquait que les données des drones de loisir utilisés sur le sol américain étaient captées par le gouvernement chinois pour s'informer sur les infrastructures stratégiques et les forces de l'ordre[5]. Cette accusation s'appuie sur le fait que ces machines enregistrent automatiquement leurs images dans des clouds auxquels le pouvoir chinois pourrait avoir accès.

1. Hugo Bonnaffé, « La goutte DDoS n'a pas fait déborder le VAC », blog d'OVH, 5 octobre 2016.
2. Une attaque « botnet » désigne une technique d'attaque par la mobilisation de machines infectées et contrôlées à distance par un pirate.
3. À ce sujet, voir la *Revue stratégique de cyberdéfense* publiée par le Secrétariat général de la défense et de la sécurité nationale, rendue publique en février 2018.
4. L'Immigration and Customs Enforcement est le bureau de l'immigration et des douanes des États-Unis.
5. Paul Mozur, « Drone Maker DJI May Be Sending Data to China, US Officials Say », *New York Times*, 29 novembre 2017.

Cette péripétie sino-américaine aux couleurs de *soft power* a été révélée quelques semaines après une autre alerte de sécurité liée à l'usage d'objets connectés. En août 2017, la Food and Drug Administration, autorité régulant la commercialisation des médicaments aux États-Unis, a ordonné la mise à jour de près de 500 000 pacemakers implantés sur des patients, dont 40 000 en France[1]. Cette décision n'était pas liée à un défaut de fabrication, ce qui est malheureusement habituel dans la production industrielle, mais à la découverte de failles de sécurité pouvant permettre à un tiers de « modifier les commandes du pacemaker, ce qui pourrait nuire au patient en vidant rapidement la batterie ou en imposant un rythme cardiaque non approprié[2] ». Si la connexion des objets, notamment médicaux, offre de merveilleuses possibilités de progrès partagé, elle recèle son lot de vulnérabilités et de dangers potentiels.

On rétorquera que la question de la dépendance des utilisateurs au système est consubstantielle au principe même du Web. Et que d'ailleurs, si une inquiétude devait être exprimée, elle devrait relayer les révélations de Bruce Schneier sur la faillibilité du réseau, laissant à penser que « quelqu'un est en train d'apprendre à détruire Internet[3] ». Selon ce spécialiste de la cybersécurité, les tentatives pour bloquer la totalité du Web par des attaques massives de déni de service sur des opérateurs essentiels d'Internet sont de plus en plus fréquentes et inquiétantes. Mais cette perspective d'un grand chaos ne doit pas nous faire oublier ce qu'il est possible de faire dès à présent pour garantir un minimum de résilience dans une société hyperconnectée. Et pour retrouver un peu de maîtrise dans l'univers du numérique.

1. Damien Leloup, « Des porteurs de pacemakers piratables incités à effectuer une mise à jour logicielle », *Le Monde*, 1er septembre 2017.
2. *Implantable Cardiac Pacemakers by Abbott: Safety Communication – Firmware Update to Address Cybersecurity Vulnerabilities*, US Food & Drug Administration, 29 août 2017.
3. Bruce Schneier, « Someone Is Learning How to Take Down the Internet », site Schneier on Security, 13 septembre 2016.

DES USAGES AUX MULTIPLES CONTRADICTIONS

La transformation numérique représente sans aucun doute une étape majeure dans le développement de nos sociétés. Les gains d'interaction, de temps, de technologie et de possibilités ne sont plus à prouver. Ils ouvrent un champ des possibles inédit pour notre civilisation. Mais ce progrès considérable dans toutes les dimensions de la vie humaine contient son lot de contradictions et de confusions, dont des auteurs comme l'Américain Nicholas Carr se sont faits les sévères porte-voix[1]. Sans entrer dans le détail de leur analyse critique, il est évident que le déploiement de la révolution numérique est un puissant facteur de désordre pour les institutions, les entreprises et les citoyens. L'absence de véritable pédagogie concernant les usages digitaux aboutit en effet à des effets pénalisants et, bien souvent, à rebours des objectifs recherchés.

UNE MÉCANIQUE D'ENFERMEMENT

Il en est ainsi des logiques d'enfermement que peuvent provoquer les outils numériques. Ce paradoxe du « fil d'actualité Facebook » avait été pointé par Eli Pariser[2] dès 2011 sous la terminologie de « bulle de

1. Nicholas Carr, *Internet rend-il bête ?*, Paris, Robert Laffont, 2011.
2. Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, New York, Penguin, 2011.

filtres ». S'appuyant sur l'exemple d'une catastrophe pétrolière, il a démontré que l'utilisation d'Internet ne permettait pas tant d'« ouvrir les individus à de nouveaux horizons[1] » que de les enfermer dans leurs convictions initiales. Il a ainsi proposé à deux de ses connaissances de faire des recherches sur la firme BP sur Google. L'une a récolté principalement des informations financières sur l'entreprise. L'autre a prioritairement recueilli des données liées à la catastrophe pétrolière du golfe du Mexique en 2010. Cette absence de base commune d'informations illustre les effets de la personnalisation du Web. Une cinquantaine de critères sont utilisés par le moteur de recherche pour « adapter » les informations au profil des utilisateurs. C'est ainsi que des réponses différentes sont affichées pour une question pourtant identique.

Contrairement à leur vocation première, les moteurs de recherche comme les réseaux sociaux maintiennent les individus dans leur communauté et déforment leur perception quant à la pluralité des opinions. Dans un rapport de 2014 consacré au numérique et aux droits fondamentaux, le Conseil d'État a lui-même souligné que, si l'utilité des algorithmes pour optimiser le fonctionnement d'un certain nombre de services ne pouvait être discutée, ceux-ci engendraient un double risque pour l'exercice des libertés : « L'enfermement de l'internaute dans une "personnalisation" dont il n'est pas maître ; la confiance abusive dans les résultats d'algorithmes perçus comme objectifs et infaillibles[2]. » Si, comme 45% des Américains, vous utilisez Facebook pour vous informer[3], vous n'aurez accès qu'aux éléments filtrés au sein de votre communauté d'amis. L'utilisateur a l'illusion d'accéder à un forum totalisant les informations et les opinions alors même que ce sont les

1. *Ibid.*
2. *Étude annuelle 2014-2014 – Le numérique et les droits fondamentaux*, Conseil d'État et juridiction administrative, 9 septembre 2014.
3. Elisa Shearer et Jeffrey Gottfried, « News Use Across Social Media Platforms », Pew Research Center, septembre 2017.

principes de redondance et de résonance qui gouvernent son fil d'actualité.

Cette logique d'enfermement aboutit, selon Eli Pariser, à ce que « vous vous endoctriniez vous-même avec vos propres opinions. Vous ne réalisez pas que ce que vous voyez n'est qu'une partie du tableau. Et cela a des conséquences pour la démocratie. Pour être un bon citoyen, il faut pouvoir vous mettre à la place des autres et avoir une vision d'ensemble. Si tout ce que vous voyez s'enracine dans votre propre identité, cela devient difficile, voire impossible[1]. » Cette mécanique de distorsion du réel qui s'exprime dès que vous lancez une requête sur Google a pour résultat que « les riches ne voient pas le même Internet que les pauvres[2]. »

Ce processus favorise la manipulation de l'opinion. Les travaux se sont multipliés ces dernières années pour démontrer la responsabilité des réseaux sociaux dans la diffusion de fausses nouvelles et des thèses conspirationnistes. Une étude de chercheurs du MIT publiée dans la revue *Science* en mars 2018[3] a tenté d'en mesurer scientifiquement l'ampleur. En analysant plus de 120 000 informations diffusées entre 2006 et 2017 sur Twitter, les chercheurs ont constaté que les fausses informations bénéficiaient d'une force de propagation bien plus importante que les informations réelles. La vérité mettrait six fois plus de temps qu'une fausse nouvelle à atteindre 1 500 personnes car elle aurait 70 % de chances de plus d'être relayée qu'une vraie nouvelle.

1. « You are basically indoctrinating yourself with your own views and you don't even know it. You don't know what you see is the part of the picture that reflects what you want to see, not the whole picture. And there are consequences for democracy. To be a good citizen, it's important to be able to put yourself in other people's shoes and see the big picture. If everything you see is rooted in your own identity that becomes difficult or impossible », *in* « 5 Questions with Eli Pariser, Author of 'The Filter Bubble' », *Time*, 16 mai 2011.
2. Michael Fertik, « The Rich See a Different Internet Than the Poor », *Scientific American*, 1er février 2013.
3. Soroush Vosoughi, Deb Roy et Sinan Aral, « The spread of true and false news online », *Science*, 9 mars 2018.

Une part de la responsabilité de cet effet d'entraînement serait liée à l'activité des comptes robots dont on évalue le nombre à 48 millions sur les 319 millions d'utilisateurs[1]. Ces machines ont un effet de masse qui augmente la résonance des fausses nouvelles, comme l'a dénoncé à plusieurs reprises l'essayiste Tristan Mendès-France dans ses prises de parole publiques. À ses yeux, l'univers des réseaux sociaux s'apparente à celui du film *Blade Runner*, où il semble bien difficile de faire la différence entre les humains et les réplicants.

Mais c'est aussi, selon les auteurs de l'étude, le comportement communautaire des utilisateurs qui favoriserait ces distorsions. Les fausses nouvelles bénéficieraient d'abord d'une circulation en vase clos, mais aussi d'un réflexe des utilisateurs consistant à privilégier des informations venant confirmer leurs opinions. La rumeur se trouve ainsi confortée face à une vérité moins sensationnelle, moins attrayante et donc moins audible. Cette logique d'enfermement est également accentuée par le recours par les entreprises à des algorithmes visant à « prédire » les souhaits de leurs clients. Plus rien d'aléatoire ne vient perturber le parcours d'une personne qui se connecte à Amazon. Le temps passé sur chaque page, les achats précédents, le profil sociologique permettent de faire défiler sur l'écran de chacun des suggestions d'achat pertinentes. Le traitement de sa masse de données permet ainsi à l'entreprise américaine de prévoir le comportement des consommateurs. Voire de le devancer.

C'est la finalité d'un brevet, évoqué par le *Wall Street Journal*[2], qui propose une méthodologie permettant de lancer la livraison d'un produit avant même que le client ne confirme son achat. Cette livraison anticipée imaginée par Amazon s'organise à partir d'un jeu d'algorithmes

1. Soroush Vosoughi, Deb Roy et Sinan Aral, « The Spread of True and False News Online », *Science*, 9 mars 2018.
2. Greg Bensinger, « Amazon Wants to Ship Your Package Before You Buy It », *The Wall Street Journal*, 17 janvier 2014.

particulièrement puissant et vise à réduire ses coûts logistiques comme ses délais de livraison. Elle constitue surtout l'aboutissement d'une rationalité économique qui dompterait définitivement les aléas humains. Par ces outils, ce sont donc des œillères que les entreprises du numérique tentent de placer sur nos visages. Et pour éviter toute distraction sur le chemin de la consommation, les sollicitations sont constantes.

DES EFFETS DE SATURATION

Ce passage de la persuasion à la captation des individus est au cœur de l'économie de l'attention étudiée par Yves Citton[1]. La surabondance d'informations permise par la révolution numérique a fait de notre capacité à être interpellés le principal enjeu économique de l'univers numérique. La valeur ne se situerait plus dans la production du bien, mais dans sa réception. C'est là une illustration supplémentaire du passage d'une économie du bien à une économie d'usage. L'enjeu consiste à favoriser la captation de l'attention, en produisant des contenus ou des outils qui suscitent la réaction. Notifications *push*, *autoplay*[2]… : au contact des écrans, notre cerveau traverse une jungle où chaque liane tente de l'attraper, même un court instant. Le même mécanisme est à l'œuvre dans les séries télévisées, qui construisent leurs scénarios sur un continuum de stimulations par la succession de changements de plans. Ce n'est d'ailleurs par nouveau et cela avait été

1. Yves Citton (dir.), *L'Économie de l'attention*, Paris, La Découverte, 2014.
2. Plusieurs outils sont utilisés sur Internet pour interagir directement avec l'utilisateur. Les notifications *push* sont des messages d'alerte s'affichant directement sur le terminal informatique ou téléphonique. L'*autoplay* est un mode d'affichage publicitaire vidéo qui permet de faire démarrer la lecture sans intervention préalable de l'internaute.

dénoncé dès l'émergence des mass media. Mais, sous l'effet de l'hyper-connexion, l'économie de l'attention change de dimension, voire de nature.

Ce sont les travaux du psychologue Daniel Kahneman qui ont popularisé l'utilisation de ces biais comportementaux dans les stratégies commerciales des GAFAM. Pour populariser ses théories, le chercheur a d'ailleurs organisé en 2007 une master class intitulée « *Thinking about thinking*[1] ». Dans l'auditoire se côtoyaient les dirigeants des principales firmes du numérique : Jeff Bezos (Amazon), Larry Page (Google), Sergey Brin (Google), Nathan Myhrvold (Microsoft), Sean Parker (Facebook), Elon Musk (SpaceX, Tesla), Evan Williams (Twitter) ou encore Jimmy Wales (Wikipedia)… L'exploitation des principes de la captation de l'attention sur les interfaces numériques de ces sociétés leur a donné un caractère industriel favorisant ce que certains n'hésitent pas à qualifier de « capitalisme mental[2] ». Sans éthique, ces techniques de « captologie » provoquent une pollution mentale préoccupante par leur intensité comme par leurs effets de long terme sur les utilisateurs. Ces sollicitations permanentes poussent au développement de comportements addictifs et compulsifs. Au point d'affaiblir inéluctablement notre capacité d'attention. Selon Microsoft, alors qu'au début du siècle la durée d'attention moyenne d'un humain était estimée à 12 secondes, quinze années plus tard, elle n'est plus que de 8 secondes. Soit l'équivalent de celle d'un poisson rouge[3].

Si cette difficulté à maintenir sa concentration est préoccupante, elle n'est pas la seule conséquence néfaste de cette chasse à l'attention menée par les réseaux sociaux. De nombreux chercheurs ont démontré que des formes d'addiction pouvaient se développer chez les jeunes

1. Tamsin Shaw, « Invisible Manipulators of Your Mind », *The New York Review Books*, 20 avril 2017.
2. Georg Franck, « Capitalisme mental », *Multitudes*, n° 54, 2013, pp. 199-213.
3. Données de Microsoft citées par Lorraine de Foucher, « Ces "pirates" qui captent votre temps de cerveau disponible », *Le Monde*, 22 septembre 2017.

publics, posant un véritable sujet de santé publique[1]. Ces effets ont été dénoncés en janvier 2018 dans une lettre ouverte adressée au patron de Facebook par l'organisation américaine Campaign for a Commercial-Free Childhood[2]. Cette dernière soulignait que les jeunes utilisateurs passant six à neuf heures par semaine sur les réseaux sociaux auraient 47 % de chances d'être plus malheureux que leurs autres camarades[3].

Ces flux continus d'informations ne sont pas seulement addictifs. Ils entament aussi la capacité à arbitrer entre ce qui est utile et ce qui ne l'est pas. Tout se vaut car tout est diffusé avec une intensité et une durée similaires. Et l'on finit, à défaut de s'y perdre, par y perdre la raison. Cette saturation cognitive amène à ne plus prendre conscience de son propre comportement numérique par une forme de cécité attentionnelle. Et à s'engager soi-même dans une course à l'attention de sa propre communauté, une course aux clics. Une information ne valant que par l'attention qu'elle récolte, les utilisateurs des réseaux sociaux ne peuvent rassurer leur ego que par le nombre de réactions que leurs publications suscitent. On twitte. On poste. On cherche l'image ou le commentaire qui feront réagir. Et l'on guette de manière addictive le nombre de likes dont on pourra publiquement se prévaloir.

C'est précisément l'inventeur de cette fonctionnalité de Facebook, le « like », qui a eu les mots les plus tranchants sur les conséquences de ces nouveaux comportements. « La dynamique de l'économie de l'attention est structurée pour compromettre la volonté humaine[4] », explique Justin Rosenstein dans un entretien accordé au *Guardian* en octobre 2017. Car, de l'exploitation du big data à partir des données

1. Sherry Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other*, Basic Books, 2011.
2. Disponible sur leur site internet.
3. E. McDool, P. Powell, J. Roberts et K. Taylor, « Social Media Use and Children's Wellbeing », *IZA Discussion Paper* n° 10412, Bonn, Institute for the Study of Labor, cité in *ibid*.
4. Paul Lewis, « "Our minds can be hijacked": the tech insiders who fear a smartphone dystopia », *The Guardian*, 6 octobre 2017.

personnelles à l'économie de l'attention, c'est bien la souveraineté numérique de chacun qui se trouve entamée. L'adoption des nouvelles technologies sans aucun frein dans les usages a réduit les capacités de libre arbitre en flattant les passions pour faire taire nos raisons.

Comme l'évoque Tristan Harris, ancien cadre chez Google qui a depuis fondé le Center For Humane Technology, avec les nouvelles technologies, « tous nos esprits peuvent être détournés. Nos choix ne sont pas aussi libres que nous le pensons[1]. » Cet effacement de la maîtrise individuelle dans le tumulte technologique pose des questions philosophiques et démocratiques dont se sont emparés Yves Citton et d'autres chercheurs travaillant avec lui. Ils plaident pour le passage d'une économie de l'attention à une écologie de l'attention[2]. Cet effacement, par son intensité, obère aussi les gains de productivité et les améliorations des conditions de travail des salariés espérés. Au point d'ailleurs de provoquer des comportements de plus en plus répandus visant à se « déconnecter » de tous les réseaux pour retrouver une part de souveraineté, mais aussi pour une efficacité accrue.

L'ACCENTUATION DES CONFUSIONS

Nous avons évoqué la profusion de courriels qui aujourd'hui complexifie la recherche de gains de productivité dans les communautés professionnelles. Chaque salarié reçoit en moyenne 88 courriels par jour et en envoie 34[3]. L'afflux d'informations bouscule la perception de

1. Cité in *ibid*.
2. Yves Citton, *Pour une écologie de l'attention*, Paris, Seuil, 2014.
3. *Email Statistics Report*, Radicati Group, mars 2015.

ce qui est prioritaire ou urgent. Les messages perturbent le travail mais transforment aussi le rapport que nous entretenons avec lui. Le principe de précaution est ainsi devenu la pratique dans l'entreprise : « En écrivant, je me protège, je me couvre[1] », remarque Guillaume Villemot. À défaut, parfois, d'être efficace puisque, comme le révèlent les travaux de Michael C. Mankins et Eric Garton[2], un salarié qui répondrait à ses courriels en réunion perdrait une dizaine de points de QI, pour atteindre la même capacité de concentration qu'en sortant d'une nuit blanche…

La numérisation a aussi gommé les frontières entre vie privée et vie professionnelle. Selon une étude d'Abode sur les pratiques numériques des salariés réalisée en 2016, neuf Européens sur dix consultent leurs courriels personnels au travail. Dans le sens inverse, près de huit Européens sur dix consultent leurs courriels professionnels en dehors des heures de travail[3]. Accentuée par la mise en place du télétravail dans de nombreuses organisations, cette simultanéité des rôles professionnels et privés serait la marque du progrès. Elle réduirait le temps perdu dans les transports, assurerait la continuité des échanges et renforcerait le bien-être des salariés. Dans cette mécanique qui se veut vertueuse, l'individu se trouve cependant enfermé dans un univers unidimensionnel qui, pour reprendre les analyses de Herbert Marcuse, intègre toutes les dimensions de l'existence privée et publique. Les travaux du philosophe sur une domination technologique s'imposant comme un processus social offrent un regard très contemporain sur les spécificités de l'hypermodernité[4]. Nos sociétés connectées se

1. Guillaume Villemot, *Le Pouvoir des mots. Osez les conversations*, Paris, Eyrolles, 2017.
2. Michael C. Mankins et Eric Garton, *Time, Talent, Energy: Overcome Organizational Drag and Unleash Your Team's Productive Power*, Harvard Business Review Press, mars 2017.
3. John Watton, « Adobe Email Survey 2016: Europeans are still addicted to email, but are easily disengaged with email campaigns », site d'Adobe, octobre 2016.
4. Denis Collin, *Comprendre Herbert Marcuse*, Paris, Max Milo, coll. « Comprendre/Essai graphique », 2017.

caractérisent par l'intégration croissante de tous les pans de vie dans un même système, en permettant notamment que la « chambre à coucher soit ouverte aux communications de masse[1] ». 42 % des Français consultent déjà leurs courriels dans leur lit[2]. Et presque la moitié de nos concitoyens n'éteignent jamais leur smartphone[3]… Il devient alors impossible de distinguer ce qui relève de la vie intime, du domaine du travail ou de la consommation.

Ce sont ainsi plus de 80 % des cadres français qui se connectent sur leur temps de loisir pour s'assurer qu'il n'y a pas de problème au travail en leur absence[4]. Ces réflexes sont alimentés par les facilités que procurent aujourd'hui les nouvelles technologies et encouragés par l'idée très répandue qu'il s'agit là d'un confort de vie. Comme Herbert Marcuse l'écrivait déjà en 1968, « si les individus se retrouvent dans les objets qui modèlent leur vie, ce n'est pas parce qu'ils font la loi des choses, mais parce qu'ils l'acceptent – non comme une loi physique mais en tant que loi de leur société[5] ». Le salarié peut conjuguer technologiquement sa vie et son travail. Mais ces réflexes obèrent les délimitations nécessaires entre les multiples facettes de l'activité humaine. Non seulement ces confusions peuvent provoquer des dégâts personnels sur l'organisation de sa propre vie, mais elles empêchent de discerner non seulement quand, mais « d'où » l'on parle.

Cette confusion des temps de vie à l'œuvre dans le monde entier amène à mettre en place dans nos législations un nouveau « droit à la déconnexion » permettant aux salariés de ne pas être contactés par leur employeur hors de leur temps de travail. En France, après son évocation

1. Herbert Marcuse, *op. cit.*
2. John Watton, « Adobe Email Survey 2016: Infographics », site d'Adobe, 3 octobre 2016.
3. Étude CSA pour l'Observatoire Bouygues Telecom des pratiques numériques des Français, 1er février 2018.
4. Étude Ifop pour Securex, *Les Cadres et l'hyperconnexion*, mai 2016.
5. Herbert Marcuse, *op. cit.*

dans le rapport Mettling sur la transformation numérique[1], c'est l'article 55 de la loi Travail du 21 juillet 2016 qui l'a consacré. Cette volonté de mettre fin au débordement des sollicitations professionnelles par les nouvelles technologies avait déjà conduit de grandes entreprises à imposer ce type de règle. Depuis 2011, Volkswagen désactive pour une partie de ses salariés l'accès aux messageries professionnelles de 18 h 15 à 7 heures en semaine[2]. À la suite d'une étude menée avec l'Univer-sité de Heidelberg sur les usages numériques, Daimler, de son côté, a instauré la possibilité pour les salariés d'activer la fonction « Mail on holiday », supprimant automatiquement les courriels reçus en période de congés et assurant leur réexpédition sur l'adresse d'un autre interlocuteur[3].

Cette confusion entre vie privée et vie publique s'exprime aussi, d'une certaine manière, dans la nature même de l'usage des messageries professionnelles. La Cour européenne des droits de l'homme (CEDH) s'est saisie récemment de la question de l'utilisation d'une boîte de courriels professionnelle à des fins privées. En septembre 2017, par une décision qui fera jurisprudence, la juridiction a acté qu'il appartenait à l'employeur de justifier la surveillance des messages électroniques par des raisons précises et d'informer au préalable le salarié de l'étendue et des modalités de ce contrôle. Mais ce que souligne aussi la CEDH, c'est que « les instructions d'un employeur ne peuvent pas réduire à néant l'exercice de la vie privée sociale sur le lieu de travail[4] ». Si l'on doit se féliciter de cette décision, celle-ci induit

1. Bruno Mettling, *Transformation numérique et vie au travail*, Ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social, septembre 2015.
2. Céline Mordant, « Droit à la déconnexion : ce que font (ou pas) les entreprises pour lutter contre l'invasion des mails professionnels », *Le Monde*, 13 mars 2016.
3. Camille Le Tallec, « Daimler donne à ses salariés les moyens de "décrocher" », *La Croix*, 1er avril 2014.
4. Arrêt de la Cour européenne des droits de l'homme, Barbulescu c. Roumanie, 61496/08, Grande Chambre, 5 septembre 2017.

l'idée qu'aujourd'hui une messagerie aurait un double usage, donc une double identité, l'une privée, l'autre professionnelle. C'est conforme aux pratiques, mais cela peut interroger sur le mélange des outils, et donc des informations.

La numérisation expose aussi à des mésusages, par maladresse ou méconnaissance. D'un point de vue médiatique, Éric Besson aura été l'un des premiers à se distinguer en confondant la fonction d'envoi d'un message privé avec celle d'un tweet. En 2011, alors ministre, il avait publié par erreur sur le réseau social un message destiné à sa compagne : « Quand je rentre, je me couche. Trop épuisé. Avec toi ? » Depuis, chacun a pu être confronté aux risques du mélange numérique où à partir du même terminal, et quelquefois d'une même application, il est possible d'utiliser – et donc de confondre – plusieurs canaux d'information. Est-ce uniquement la preuve qu'un apprentissage des outils numériques s'impose ? Difficile de n'y voir que cela quand on connaît les mésaventures de certaines grandes entreprises. En 2011, le compte Twitter d'un des personnages fictifs des campagnes publicitaires de Sony, Kevin Butler, a accidentellement retweeté le code de déverrouillage de la PS3, en le confondant avec des coordonnées pour couler un porte-avions à la bataille navale[1]. En juillet 2017, Apple a révélé le design de l'iPhone 8 en laissant des fichiers accessibles dans le logiciel d'exploitation de son enceinte HomePod[2].

Dans les faits, la multiplicité des canaux favorise les méprises et les erreurs. Un *multitasker*, pour reprendre un terme à la mode[3], ferait

1. « Sony accidentally retweets PS3 "jailbreak" code, mistakes it for a "Battleship" reference », *Digital Trends*, 2 septembre 2011.
2. Étienne Combier, « Apple victime d'une fuite majeure avant la sortie des nouveaux iPhone », *Les Échos*, 12 septembre 2017.
3. Issu du vocabulaire informatique, « *multitasker* » est un terme anglophone qui désigne un système capable de traiter en même temps plusieurs programmes. Il est utilisé pour qualifier les salariés qui exécutent parallèlement de multiples tâches.

50 % d'erreurs supplémentaires dans l'exécution de ses tâches de travail, même si les conséquences ne sont pas nécessairement dramatiques[1]. Pour résumer, on diffuse n'importe quelle information sur n'importe quel support numérique. Et si, dans des temps pas si anciens, il était possible de se tromper d'interlocuteur en composant un numéro de téléphone, reconnaissons que les risques ont changé de nature lorsqu'on s'engage à « répondre à tous » au lieu de privilégier la réponse unique ou que l'on publie un message privé sur son mur Facebook…

1. John Medina, *Brain Rules: 12 Principles for Surviving and Thriving at Work, Home, and School*, Seattle, Pear Press, 2008.

RETROUVER LA MAÎTRISE ET INSTAURER UNE ÉTHIQUE NUMÉRIQUE PARTAGÉE

Nous avons vu que la numérisation imprègne toute la société sans avoir été civilisée. Les interrogations fondamentales peinent à trouver leur place dans les mutations en cours. Il est donc temps d'édifier de nouveaux piliers de confiance. Pour ne pas perdre pied dans la révolution numérique, les utilisateurs doivent pouvoir se réapproprier les outils et sécuriser les informations échangées. Il s'agit de remettre de l'ordre pour sortir de l'anarchie.

NE PLUS PERDRE PIED

Avec Internet, une donnée produite devient largement accessible. C'est un élément fort de progrès et de transparence. Mais elle doit aussi pouvoir être supprimée dans des conditions déterminées. C'est une nécessité éthique. L'idée d'une juste articulation entre droit à l'information et droit à l'oubli fait ainsi l'objet de discussions au sein de la Cour de justice de l'Union européenne (CJUE). En février 2017, celle-ci a été saisie par le Conseil d'État sur l'application du droit au déréférencement[1], dont le principe avait été acté dès 2014 dans un arrêt

1. Décision du Conseil d'État, Mme C, M. F, M. H, M. D, 24 février 2017.

Google Spain[1]. Dans sa décision, la CJUE a reconnu le droit pour les utilisateurs de demander à un moteur de recherche, sous certaines conditions, de supprimer des résultats affichés à partir d'une requête sur leur propre nom.

Plus largement, cette maîtrise des données échangées passe par une application stricte des finalités de leurs usages. À cet égard, une avancée majeure va avoir lieu avec l'application dès le 25 mai 2018 du Règlement général sur la protection des données (RGPD). Celui-ci offre un éclairage nouveau sur les enjeux liés à la protection des données. Il renforce l'obligation pour tout responsable de traitement de n'exploiter des données que dans le cadre d'une finalité définie. Ce principe de minimisation oblige à recueillir le consentement explicite des personnes concernées et à détruire les données une fois la finalité atteinte.

Cette réglementation est nécessaire pour s'assurer qu'une donnée ne peut être détournée de son usage, au détriment de la personne qui la produit. Prenons l'exemple du suivi des consommations d'eau d'un particulier. Celui-ci a tout intérêt à utiliser un service qui peut lui permettre, par un échange de données, de maîtriser sa facture et offre à son opérateur la possibilité de déceler d'éventuelles fuites. Mais aurait-il intérêt à ce que l'information soit transmise à sa mutuelle si elle mettait en évidence son état diabétique et occasionnait une surprime d'assurance du fait qu'il tire plusieurs fois la chasse d'eau durant la nuit ? Le risque de diffusion de données sensibles a déjà conduit la Commission nationale de l'informatique et des libertés (CNIL) à rendre publique sa mise en demeure de l'Assurance-maladie concernant la sécurisation des données médicales. Dans sa

1. Arrêt de la Cour de justice de l'Union européenne, « Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González », 13 mai 2014.

communication du 27 février 2018[1], elle souligne les fragilités du fichier SNIIRAM[2] qui regroupe des milliards de données relatives à la santé des assurés sociaux. On parle ici des actes médicaux, des feuilles de soins et des séjours hospitaliers ! Cette base de données ne garantirait pas l'anonymat des assurés. Elle pourrait subir l'intrusion de tiers, et la sauvegarde des informations en cas d'attaque de l'infrastructure informatique ou d'incident ne serait pas garantie…

Applicable à tous – institutions, entreprises, associations, syndicats dans l'Union européenne, mais aussi un grand nombre d'entreprises situées hors de l'Europe mais proposant des services à des résidents de l'UE –, le nouveau règlement européen suscite l'anxiété s'agissant de sa mise en œuvre. 86 % des entreprises s'inquiètent des conséquences possibles d'un défaut de conformité et près de la moitié craignent de ne pas être prêtes à temps[3]. Mais, par les obligations qu'elle impose, cette réglementation ne constitue pas tant une accumulation étouffante de contraintes qu'une mise en lumière salutaire des enjeux liés à l'économie des données et à la numérisation. Par les sanctions qu'elle prévoit, elle oblige à la maîtrise des usages et décloisonne ces problématiques historiquement dévolues aux seuls responsables des systèmes d'information. Elle en fait une question – et une responsabilité – transversale pour toute entité.

Par cette démarche volontariste, l'Union européenne contribue au nécessaire recul des incertitudes liées aux usages numériques. C'est pourquoi il convient d'accompagner ce mouvement, en plaidant pour la démocratisation de solutions garantissant des échanges sécurisés.

1. « SNIIRAM : la CNAMTS mise en demeure pour des manquements à la sécurité des données », communiqué de la CNIL, 27 février 2018.
2. Le SNIIRAM est le Système national d'information interrégime de l'Assurance-maladie. Il a été créé par la loi du 23 décembre 1998 pour moderniser les activités de la CNAMTS (Caisse nationale de l'Assurance-maladie des travailleurs salariés).
3. Rapport Veritas, GRPD, juillet 2017.

Issues des pratiques de la cyberdéfense, plusieurs initiatives ont été engagées pour offrir de nouvelles modalités de communication simples et gratuites. Elles doivent être popularisées pour offrir une solution autre que la logique agrégative des GAFAM, bien sûr, mais aussi pour prévenir la perte de confiance des utilisateurs. En effet, si cette confiance est déjà entamée en raison de la désappropriation qu'engendre l'exploitation des données, elle pourrait être encore affaiblie du fait des mauvais usages qui sont faits des nouvelles technologies.

Du côté des pouvoirs publics, d'importants efforts ont été réalisés ces dernières années pour mettre en œuvre la transformation numérique des services publics. Dès 2016, 66 % des Français ont pu accomplir des démarches administratives par Internet[1], et le gouvernement a fixé le proche horizon de 2022 comme échéance pour que l'intégralité des services publics soient dématérialisés[2]. Mais, dans cette marche forcée nécessaire, la compréhension des enjeux de la numérisation est encore loin d'être partagée. Dans une étude publiée en 2015, *La Gazette des communes* révélait que 50 % des sites internet des communes n'étaient pas mis à jour et restaient mal sécurisés[3]. Or, si une présence sur le Web est précieuse, a fortiori pour des institutions, elle peut s'avérer pénalisante si elle n'est pas pensée, adaptée et entretenue. Une commune a peu de chances d'offrir une image positive à des usagers visitant son portail internet figé depuis des années… Et une entreprise n'a pas davantage de chances d'améliorer son e-réputation si elle multiplie l'ouverture de comptes sur les réseaux sociaux sans en faire

1. Baromètre Digital Gouv' 2016 Sopra Steria et Ipsos.
2. Sylvain Rolland, « L'État 100 % numérique de Macron coûtera 9,3 milliards d'euros », *La Tribune*, 26 septembre 2017.
3. Julien Kirch et Sabine Blanc, « Plusieurs milliers de sites internet de communes mal sécurisés », *La Gazette des communes*, 25 mars 2015.

usage… La domestication des outils digitaux doit donc devenir une priorité publique. De la même façon que l'éducation à l'image s'est développée pour favoriser un rapport apaisé et rationnel à l'audiovisuel, des initiatives massives doivent être engagées pour permettre à chacun de maîtriser – autant que faire se peut – la révolution numérique[1].

D'aucuns y verront des obstacles malvenus au déploiement du progrès. Il s'agit tout au contraire de permettre à nos sociétés de se déployer dans les champs ouverts par le numérique en connaissant ses règles, mais aussi ses dangers. Car il n'est pas dit que demain, dans cette anarchie, la confiance dans le numérique simplement adossée à des effets de réseaux ne s'effondrera pas dans une même logique.

PROTÉGER LA DÉMOCRATIE

Avant que cette confiance dans les acteurs du numérique ne s'effondre, il convient de prendre la mesure de leur influence dans le jeu démocratique. Le numérique est le principal vecteur d'informations des citoyens. Or, nous avons vu à quel point le déterminisme était exacerbé par l'usage d'algorithmes fondés sur les comportements des consommateurs.

Évidemment, la multitude des données nécessite un traitement et une hiérarchisation pour en démêler la richesse. C'est la loi du Web. Mais, en éloignant l'aléatoire de toute recherche, en favorisant les récurrences et en agrégeant les données personnelles, la mécanique de l'Internet exerce une influence inégalée sur les choix individuels. La

1. Sur ce sujet, il faut signaler l'initiative personaldata.io. Il s'agit d'une plateforme citoyenne facilitant les demandes d'accès aux données détenues par des tiers.

possibilité d'anticiper des comportements ouvre la voie à une manipulation des choix des individus permettant de passer d'une algorithmie prédictive à une algorithmie prescritive. Cela signifie que les données peuvent être exploitées non plus seulement pour prévoir un comportement individuel, mais pour l'influencer. C'est la conviction sur laquelle s'est fondé le succès de l'entreprise Cambridge Analytica, qui a joué un rôle déterminant dans la dernière élection présidentielle américaine en 2016 comme dans la consultation britannique sur le Brexit la même année.

Comme l'explique le journaliste et documentariste Thomas Huchon dans un documentaire consacré à la campagne électorale de Donald Trump[1], ce sont les travaux du psychologue Michal Kosinski qui ont favorisé ces nouvelles approches de propagande électorale. Tout a commencé par le déploiement sur Facebook d'un test gratuit de personnalité dénommé myPersonality. Cette application a connu un succès important et permis de condenser les profils psychologiques de 6 millions de personnes à leur insu[2] ! Une fois encore, c'est le fait que les utilisateurs n'étaient pas conscients de la valeur des informations qu'ils partageaient qui a été le point de départ. La gratuité du service a masqué la dépossession des données personnelles qu'il allait provoquer. Cette base de données a été régulièrement enrichie pour améliorer les algorithmes. En janvier 2015, les chercheurs publient leurs résultats. Le spécialiste Jean-Paul Crenn a expliqué par la suite : « Les algorithmes de Kosinski et de son équipe sont capables d'évaluer le profil psychologique d'une personne et ainsi de prédire son comportement, mieux que ses collègues sur la base de l'analyse de 10 likes sur Facebook. 70 likes sont suffisants pour en savoir plus que

1. Thomas Huchon, *Unfair Game : comment Trump a manipulé l'Amérique*, 2017.
2. « myPersonality database », site de l'Université de Cambridge.

les amis de la personne, 150 ses parents, 300 son conjoint. Plus de likes peuvent même surpasser ce qu'une personne pense savoir… d'elle-même[1]. » Dans les années qui suivent, Cambridge Analytica applique cette puissance d'analyse à la population américaine. Il dresse le profil psychométrique[2] de 220 millions de personnes[3] par le croisement des données récupérées sur les réseaux sociaux, celles du registre des historiques d'achat par carte de crédit ou encore des propriétaires d'armes à feu. Ce trésor inestimable a été mis au service de l'équipe numérique de Donald Trump sous l'impulsion d'Alexander Nix, président de Cambridge Analytica, qui a ainsi pu envoyer les messages personnalisés nécessaires pour influencer les votes des électeurs.

Ce que Cambridge Analytica a été capable d'accomplir a eu un formidable retentissement médiatique à la suite du témoignage de l'un de ses anciens employés, Christopher Wylie. Ses révélations, accompagnées d'une enquête détaillée du *Guardian*, du *New York Times*[4] et de *The Observer*, ont pointé la responsabilité de Facebook dans la récolte et l'exploitation par la société incriminée des données de 87 millions de ces utilisateurs[5]. Par le biais d'un test de personnalité accessible sur la plateforme et présenté comme une application universitaire utilisée par des psychologues, il a été possible d'agréger non seulement des informations sur les personnes qui avaient répondu au questionnaire, mais aussi sur leurs réseaux d'amis. Par ce stratagème,

1. Jean-Paul Crenn, « Algorithmes prédictifs : au cœur de la politique ? », *Revue de la gendarmerie nationale*, n° 260, décembre 2017.
2. Le profil psychométrique d'un individu permet de déterminer ses comportements et caractéristiques particulières et de les comparer à une population de référence. Il est notamment utilisé dans le secteur des ressources humaines pour accompagner des processus de recrutement.
3. Nina Burleigh, « How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters », *Newsweek*, 8 juin 2017.
4. « How Trump Consultants Exploited the Facebook Data of Millions », *New York Times*, 17 mars 2018.
5. Mike Schroepfer, directeur de la technologie de Facebook, « An Update on Our Plans to Restrict Data Access on Facebook », 4 avril 2018.

« nous nous sommes servis de Facebook pour récupérer les profils de millions de personnes. Nous avons ainsi construit des modèles pour exploiter ces connaissances, et cibler leurs démons intérieurs[1] », détaille Christopher Wylie.

Si ce scandale a pu mettre au jour les failles éthiques du réseau social incarné par Mark Zuckerberg, il illustre surtout les potentialités d'instrumentalisation des outils numériques de communication à des fins politiques. La société Cambridge Analytica s'était spécialisée dans la mise en œuvre de « PsyOps » pour ses clients. Il s'agissait d'opérations psychologiques permettant de manipuler l'opinion. Et, comme le relève le mathématicien Paul-Olivier Dehaye, « l'un des endroits les plus efficaces pour faire cela, c'est Facebook[2] ». Cette plateforme ne permet pas seulement de manipuler les individus, mais tout le réseau, toute la circulation de l'information. C'est l'organisation même de ces outils, avec leur logique de communautés, d'enfermement comme de sursollicitation, qui permet d'exploiter à une échelle inédite et avec des moyens inégalés les informations récupérées sur chaque citoyen.

Certes, les partis politiques ont toujours adapté leurs discours aux différents publics. On ne diffuse pas le même tract devant une maison de retraite ou une université. Mais l'émergence du big data et des réseaux sociaux a changé radicalement l'échelle du profilage et l'impact que celui-ci peut avoir sur nos démocraties. On peut évoquer deux raisons à cela. La première est que ce mouvement s'accompagne, comme nous venons de le montrer, de potentialités inégalées de manipulation massive de l'opinion. La connaissance des habitudes de

1. « We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons », propos de Christopher Wylie cités dans Carole Cadwalladr et Emma Graham-Harrison, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *The Guardian*, 17 mars 2018.
2. Jérôme Hourdeaux, « Facebook s'embourbe dans le scandale Cambridge Analytica », Mediapart, 21 mars 2018.

chacun, mais aussi la confusion sur l'identité et les inconnues sur la crédibilité des émetteurs de messages permettent de distordre la réalité et d'influencer les choix dans des proportions inégalées. Les modèles prédictifs fondés sur le big data permettent en effet de prévoir les conséquences comportementales qu'aurait l'envoi d'un message d'un certain type, à une certaine heure, sur un public spécifique. Ce sont des encouragements à la diffusion de fausses nouvelles dont l'unique finalité est de peser sur l'opinion des cibles visées. « Si la rumeur est un phénomène aussi ancien que l'humanité, ou peu s'en faut, il est indéniable que l'essor d'Internet en a démultiplié la portée[1] », explique le philosophe Cass R. Sunstein. En effet, avec l'usage effréné de robots, la récurrence d'une information devient le moteur de sa crédibilisation. Dans le cadre des auditions menées par les commissions parlementaires américaines au sujet des *fake news* de la campagne présidentielle de 2016, Facebook a reconnu que 126 millions d'Américains avaient visionné de fausses nouvelles diffusées par des intérêts russes en vue de peser sur l'issue du scrutin[2]. Ce sont 80 000 posts sur Facebook qui auraient été publiés par de faux comptes russes[3]. Pour Twitter, on estime à plus de 36 000 le nombre de comptes qui ont généré automatiquement des informations sur l'élection américaine[4].

La seconde raison pour laquelle l'apparition du big data a changé la donne est que l'usage des données par les équipes de campagne renforce une atomisation du discours électoral déjà préoccupante pour l'idée que l'on peut se faire de la politique. L'individualisation des

1. Cass R. Sunstein, *Anatomie de la rumeur*, Genève, Éditions Markus Haller, 2012.
2. David Ingram, « Facebook says 126 million Americans may have seen Russia-linked political posts », Reuters, 30 octobre 2017.
3. « Russia-backed Facebook posts "reached 126m Americans" during US election », *The Guardian*, 31 octobre 2017.
4. Craig Timberg et Elizabeth Dwoskin, « Russian content on Facebook, Google and Twitter reached far more users than companies first disclosed, congressional testimony says », *The Washington Post*, 30 octobre 2017.

réponses politiques a été rendue nécessaire par les transformations sociales de notre époque. Pour reprendre l'analyse d'Ulrich Beck[1], celles-ci détachent les individus des rapports de classe concrets. L'acteur politique doit être capable d'adapter son discours à chacun suivant sa situation, sa place dans la société et ses attentes. Son projet collectif doit trouver un écho auprès de chaque individu, auprès de chaque électorat pour fédérer les voix. C'est ce à quoi travaillaient les stratèges de campagne, en s'appuyant sur les outils à leur disposition : études qualitatives, sondages, données sociologiques. Mais les potentialités du big data ont donné une dimension industrielle à l'individualisation du message politique.

En dehors de l'exemple américain que nous venons d'évoquer, la majorité des candidats à l'élection présidentielle française de 2017 ont eu recours à des prestataires comme NationBuilder ou au logiciel d'analyse de la start-up Liegey Muller Pons pour adresser leurs argumentaires de façon personnalisée. Si l'impact de ces outils a transformé la façon même de faire campagne, il invite à s'interroger dès lors qu'ils deviennent la règle. L'individualisation du message politique n'affaiblit-elle pas le projet collectif ? En s'adaptant de manière aussi fine à chacun, la propagande électorale contribue à l'atomisation d'une société qui peine déjà à transcender ses clivages. La capacité de dépassement du politique peut ainsi se trouver mise à mal par un marketing individualisé qui enferme l'électeur dans ses propres préoccupations et l'empêche de se hisser à la hauteur de l'intérêt général. Pour être un bon citoyen, il faut être capable de se mettre à la place des autres et avoir une vision d'ensemble, explique Eli Pariser[2]. Ce n'est pas ce que nous promettent les technologies, qui favorisent l'étroitesse de la pensée et le quant-à-soi individualiste.

1. Ulrich Beck, *La Société du risque. Sur la voie d'une autre modernité*, Paris, Aubier, 2001.
2. Eli Pariser, *op. cit*.

SORTIR DE LA CÉCITÉ ÉTHIQUE

Nous vivons aujourd'hui dans un contexte d'interdépendance complexe alimentée par la multiplication des échanges économiques et sociaux. La transformation numérique en est l'expression la plus aboutie. Cet environnement en réseaux représente un terrain de possibilités, mais recèle aussi des menaces nouvelles. Hier, les risques étaient clairement identifiables et indépendants les uns des autres[1]. Aujourd'hui, les menaces sont incertaines et s'intègrent les unes aux autres. Les risques endogènes et les transformations exogènes se nourrissent mutuellement, provoquant une perte de maîtrise qui constitue la source principale de vulnérabilité de tous les acteurs. Et sème le trouble chez de nombreux utilisateurs.

Notre dépendance aux GAFAM représente d'abord un risque technologique. S'il serait illusoire d'espérer s'affranchir brutalement des services apportés par Google, Facebook et consorts, le monopole dont jouissent ces entreprises constitue un obstacle à notre résilience collective. Pour les États comme pour les entreprises, il s'agit de trouver un équilibre entre une exposition nécessaire au monde extérieur et la préservation de leurs capacités d'action. Cette exigence d'« autonomie reliée » est une condition de leur survie face aux menaces grandissantes de contamination des systèmes. Les mécaniques d'homogénéisation inhérentes au déploiement des objets connectés portent en elles les faiblesses qui permettront leur détournement. C'est une des caractéristiques d'une société qui est passée du risque à l'incertitude, comme le démontre Gilles Hilary, professeur à l'université de Georgetown. « Dans un monde de risques, le traitement d'une menace

1. Gilles Hilary, « Nouvelles complexités, nouvelles menaces », *Revue de la gendarmerie nationale*, n° 260, décembre 2017.

de façon systématique rend le système plus sûr. Par exemple, la standardisation de la vaccination réduit les risques d'épidémies. Dans un monde d'incertitude, cette approche peut déstabiliser les systèmes. Par exemple, l'utilisation de protocoles de sécurité identiques facilite la propagation de virus[1]. »

Devant les risques cyber, la standardisation des outils et la dépendance à quelques acteurs seulement représentent donc des fragilités majeures. Qu'adviendra-t-il quand le cloud d'Amazon, qui représente plus de 30% du marché des données « en nuage[2] », connaîtra un black-out ? C'est toute l'économie qui sera paralysée. Il convient dès lors de développer une culture de la pluralité des systèmes et de prendre les mesures permettant de favoriser l'hétérogénéité du monde numérique. À cet effet, l'Union européenne doit pouvoir s'appuyer sur des infrastructures différentes – éventuellement compatibles avec les systèmes actuels, mais indépendantes. On retrouve cette préoccupation dans les recommandations formulées par Louis Gautier, alors à la tête du Secrétariat général de la défense et de la sécurité nationale (SGDSN), dans la *Revue stratégique de cyberdéfense* rendue publique en février 2018[3]. Dans les domaines particulièrement sensibles, ce risque de dépendance technologique est extrêmement préoccupant. Pour autant, relativiser l'omnipotence des acteurs du numérique reviendrait à nier les « effets de réseaux » dont ils sont les bénéficiaires.

Notre dépendance aux GAFAM constitue aussi un risque d'affaiblissement de notre souveraineté numérique. Malgré les efforts actuels de la Commission européenne, les géants du Web accumulent des données qui fondent leur richesse. L'économie de la donnée doit

1. *Ibid.*
2. « Cloud Market Keeps Growing at Over 40%; Amazon Still Increases its Share », Synergy Research Group, 27 octobre 2017.
3. *Op. cit.*

devenir un enjeu politique et faire l'objet d'un véritable débat citoyen. Si la donnée est un savoir, son exploitation ne peut être abandonnée aux simples logiques du marché. Elle constitue le capital de nos industries et le vécu de chaque citoyen. Utilisée sans consentement, elle dépossède l'identité, et donc annihile la souveraineté personnelle.

Mais, bien souvent, il s'agit d'un braquage indolore. Berné par la gratuité principielle de la nouvelle économie et floué par des opérateurs qui masquent leurs intentions derrière d'obscures conditions d'utilisation, on ne s'en aperçoit même pas. L'étude sur la patrimonialité des données publiée par le think tank GenerationLibre[1] relève à juste titre qu'il ne peut exister de consentement éclairé concernant ses propres données dès lors que celui-ci se fonde sur une profusion de contrats peu intelligibles. Un internaute américain est ainsi amené à souscrire à 1 500 conditions d'utilisation chaque année, soit l'équivalent de 76 jours de lecture en continu[2]…

C'est pourtant la liberté de chacun, sa capacité à préserver non seulement son intimité, mais ses capacités de libre arbitre qui sont en jeu. Ce sont les capacités humaines dont il est question, dans un monde où l'on peine à discerner qui, du produit ou de l'individu, est le maître ; qui, de l'individu ou du produit, a été façonné pour l'autre. Plus largement, l'ouverture des données anonymisées soulève déjà des interrogations fortes sur la répartition de la richesse qu'elle peut générer. En 2015, la loi Macron a ainsi imposé aux entreprises de transport public l'ouverture de leurs données, désormais utilisables par tous. L'intention est louable mais crée un effet d'aubaine pour les géants du numérique. Ils bénéficient gratuitement de ces données, qui

1. Lucas Léger (dir.), *Mes données sont à moi. Pour une patrimonialité des données personnelles*, GenerationLibre, 2018, www.generationlibre.eu/data-a-moi
2. Aleecia M. McDonald et Lorrie Faith Cranor, « The Cost of Reading Privacy Policies », *Journal of Law and Policy*, Carnegie Mellon University, 2009.

viennent alimenter leurs propres services. Sous l'impulsion de la SNCF, de la RATP et de BlaBlaCar, une *data warehouse* (banque de données) a donc été constituée pour tenter de maîtriser l'exploitation de ces jeux de données. Inéluctablement, les mêmes questions se poseront rapidement sur des données publiques et les risques d'exploitation privative et concurrentielle.

Les possibilités gigantesques qu'offrent les algorithmes doivent être favorisées. C'est le sens du progrès. Mais elles doivent s'appuyer sur une éthique, avec les réglementations qui s'imposent ; autant dire sur un rôle offensif de la puissance publique. Si quelques initiatives méritent d'être relevées, telle la mise en œuvre de la plateforme TransAlgo[1], reconnaissons que les pouvoirs publics peinent encore à prendre leurs responsabilités sur ces enjeux. Si, avec la multiplication des incidents, ils ont acquis de la maturité face aux cybermenaces, les infrastructures de défense et la transformation des comportements restent à la traîne dans la course technologique qui oppose les attaquants à leurs cibles. Des moyens doivent être engagés dans la durée pour répondre au défi que représente ce que la *Revue stratégique de cyberdéfense* qualifie de « Far West cybernétique » : sans intervention publique, les menaces s'agglomèrent.

La souveraineté numérique des organisations doit en effet être préservée. Tout comme celle des utilisateurs, qui doivent être sensibilisés. Il s'agit d'une grande cause nationale, et il nous faut faire en sorte qu'elle soit perçue comme telle par les citoyens. Par exemple, on peut obliger les opérateurs à informer clairement leurs clients sur l'usage commercial des informations collectées. On peut aussi s'appuyer sur la vigilance des utilisateurs. Il s'agit de l'encourager, sur le modèle

1. Coordonnée par l'Institut national de recherche en informatique et en automatique (Inria), TransAlgo est une plateforme scientifique collaborative destinée à favoriser le développement d'outils logiciels et de méthodes de tests d'algorithmes et la promotion de leur utilisation.

de l'initiative lancée en 2016 par le gouvernement (quoique de manière trop confidentielle). Le portail signalement-sante.gouv.fr permet aux citoyens de signaler tout événement sanitaire indésirable constaté, mais aussi les défauts de sécurisation de la transmission d'actes ou d'examens médicaux.

Mais, nous l'avons démontré, la souveraineté numérique ne se limite pas à une exigence de sécurité. Elle oblige à penser globalement la maîtrise de la révolution numérique, sa domestication et ses conséquences sociales, organisationnelles, économiques et psychologiques. Le numérique n'a pas seulement effacé l'espace et le temps. Il a estompé les frontières qui séparaient l'espace privé et l'espace public, distinguaient le temps personnel du temps de travail, différenciaient le virtuel et le réel. La révolution en cours a aussi bouleversé le rapport entre les acteurs économiques et les pouvoirs publics, la hiérarchie des informations et la place des fausses nouvelles, la chaîne de valeur et le rapport de production, la distinction entre ce qui doit relever de l'attention ou de l'intention.

Cette révolution produit ses propres fragilités car elle est encore dénuée d'éthique. On se plaît à considérer que la domination de la machine sur l'homme constituerait le danger suprême du progrès technologique. Mais ce n'est pas tant ce péril hypothétique que ce qui se passe aujourd'hui qui devrait nous inquiéter. Nous parlons de cette cécité éthique qui nous amène à laisser une technologie se diffuser sans en maîtriser les effets.

CONCLUSION

« Le matin du 16 avril, le docteur Bernard Rieux sortit de son cabinet et buta sur un rat mort, au milieu du palier. Sur le moment, il écarta la bête sans y prendre garde et descendit l'escalier. Mais arrivé dans la rue, la pensée lui vint que ce rat n'était pas à sa place et il retourna sur ses pas pour avertir le concierge[1]. » Bientôt, ce fut toute la ville qui se trouva submergée de rats morts.

En février 2016, la banque centrale du Bangladesh est victime d'un vol par le biais de virements frauduleux, pour plus de 80 millions de dollars[2]. Dans les jours qui suivent, les données médicales des patients d'un groupe hospitalier du nord de la France se retrouvent accessibles en ligne et consultables par tous[3]. L'été de la même année, les données personnelles de 112 000 policiers sont mises en ligne par un salarié malintentionné de la Mutuelle générale de la police[4]. En mai 2017, les réseaux informatiques du système de santé britannique sont attaqués et obligent à renvoyer temporairement des patients vers les services d'urgence[5]. L'été, deux virus successifs infectent des milliers de serveurs de grands groupes et provoquent l'arrêt total d'activités de nombre

1. Albert Camus, *La Peste*, Paris, Gallimard, 1947.
2. Raju Gopalakrishnan et Manuel Mogato, « Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat », Reuters, 19 mai 2016.
3. « Béthune : des dossiers médicaux en accès libre sur le Web depuis au moins trois jours », *La Voix du Nord*, 18 février 2016.
4. Caroline Piquet, « Les données personnelles de 112 000 policiers ont fuité sur le Web », *Le Figaro*, 27 juin 2016.
5. « Cyberattaques : les hôpitaux britanniques, principales cibles atteintes », *Les Échos*, 13 mai 2017.

d'entre eux[1]. En septembre, un fichier contenant des appréciations individuelles confidentielles sur des candidats à des piges à Radio France est diffusé par erreur à l'ensemble des candidats[2]. Le même mois, l'un des plus importants cabinets de conseil au monde, la société Deloitte, se fait pirater des données relatives à son portefeuille de clients[3]. Le mois suivant, on apprend que la fuite de données subie par l'hébergeur de courriels Yahoo en 2013 a concerné la totalité des comptes existant à l'époque… soit 3 milliards[4].

Quant à la ville d'Atlanta, elle a expérimenté en mars 2018 une nouvelle forme de « prise d'otage », selon la formule de son maire Keisha Lance Bottoms[5]. Par l'introduction d'un *ransomware* (rançongiciel) dans les réseaux informatiques de cette métropole, une équipe de pirates a pu bloquer un grand nombre de services, renvoyant les 8000 fonctionnaires à l'usage du papier et du crayon. Les forces de l'ordre ont dû écrire les rapports à la main, le tribunal municipal a été incapable de valider des mandats, les demandes d'emploi ne pouvaient plus être enregistrées, les habitants ne pouvaient plus régler leurs factures en ligne…

Dans notre révolution numérique, les cadavres s'amoncellent progressivement dans les recoins de nos villes, de nos vies. L'anxiété monte lentement dans les rues, dans les flux. Mais, telle la peste, ces menaces grandissantes restent encore impalpables. Dans l'allégresse du progrès numérique, les vulnérabilités technologiques savent se faire oublier. Elles sont tapies mais peuvent se révéler à tout moment. Des

1. À l'été 2017, les virus WannaCry et NotPetya ont endommagé de nombreuses infrastructures.
2. Alexis Delcambre, « Radio France : des commentaires sur des journalistes candidats à un concours envoyés par erreur », *Le Monde*, 25 septembre 2017.
3. Martin Untersinger, « Le géant du conseil Deloitte victime d'un piratage », *Le Monde*, 25 septembre 2017.
4. « Yahoo : les 3 milliards de comptes affectés par la cyber-attaque de 2013 », AFP, 4 octobre 2017.
5. Alan Blinder et Nicole Perlroth, « A Cyberattack Hobbles Atlanta, and Security Experts Shudder », *New York Times*, 27 mars 2018.

remèdes existent, distillés par les autorités publiques, mais ils nécessitent une prise de conscience fondée sur une éthique partagée. Car cette peste d'un nouveau genre est l'affaire de tous.

TABLE DES MATIÈRES

Introduction 5

L'effet de bascule 11

Des usages aux multiples contradictions 29

Retrouver la maîtrise et instaurer une éthique numérique partagée 43

Conclusion 59

COLLECTION DIRIGÉE PAR GILLES FINCHELSTEIN
ET LAURENT COHEN

FEPS - FONDATION EUROPÉENNE D'ÉTUDES PROGRESSISTES
Rue Montoyer 40, 4e étage
1000 - Bruxelles, Belgique
T: +32 2 234 69 00
Email : info@feps-europe.eu
Site web : www.feps-europe.eu/fr/
Twitter : @FEPS_Europe

FONDATION JEAN-JAURÈS
12 Cité Malesherbes
75009 Paris, France
T : +33 1 40 23 24 00
Email : info@jean-jaures.org
Site web : www.jean-jaures.org
Twitter : @j_jaures

AVEC LE SOUTIEN FINANCIER DU PARLEMENT EUROPÉEN
Le présent document ne représente pas les opinions du Parlement européen, mais seulement celles de son ou ses auteur-e-s.

AVERTISSEMENT : La mission de la Fondation Jean-Jaurès et de la Fondation européenne d'études progressistes est de faire vivre le débat public et de concourir ainsi à la rénovation de la pensée social-démocrate. Elles publient donc les analyses et les propositions dont l'intérêt du thème, l'originalité de la problématique ou la qualité de l'argumentation contribuent à atteindre cet objectif, sans pour autant nécessairement reprendre à son compte chacune d'entre elles.

Réalisation : REFLETS GRAPHICS

MAXIME DES GAYETS

LA GRANDE DÉPOSSESSION
POUR UNE ÉTHIQUE NUMÉRIQUE EUROPÉENNE

Piratages industriels, cyber-attaques, fuites de données, manipulations politiques, effets psycho-sociaux… : la révolution numérique révèle, jour après jour, son côté le plus obscur.
Simples aléas ? Fragilités inhérentes à toute grande transformation ? Pour Maxime des Gayets, ce serait bien plutôt l'expression d'une mécanique plus profonde de dépossession des vies, des valeurs comme des identités. En appelant ainsi à la responsabilité collective des citoyens européens, il formule des propositions pour sortir de notre aveuglement éthique à l'égard d'une technologie aux effets de plus en plus incontrôlables.

Maxime des Gayets, consultant en cybersécurité et résilience des entreprises, est conseiller régional d'Île-de-France.

ISBN : ISBN : 978-2-36244-115-8

6 €

FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES
FONDATION EUROPÉENNE D'ÉTUDES PROGRESSISTES

www.feps-europe.eu

Fondation Jean Jaurès

www.jean-jaures.org