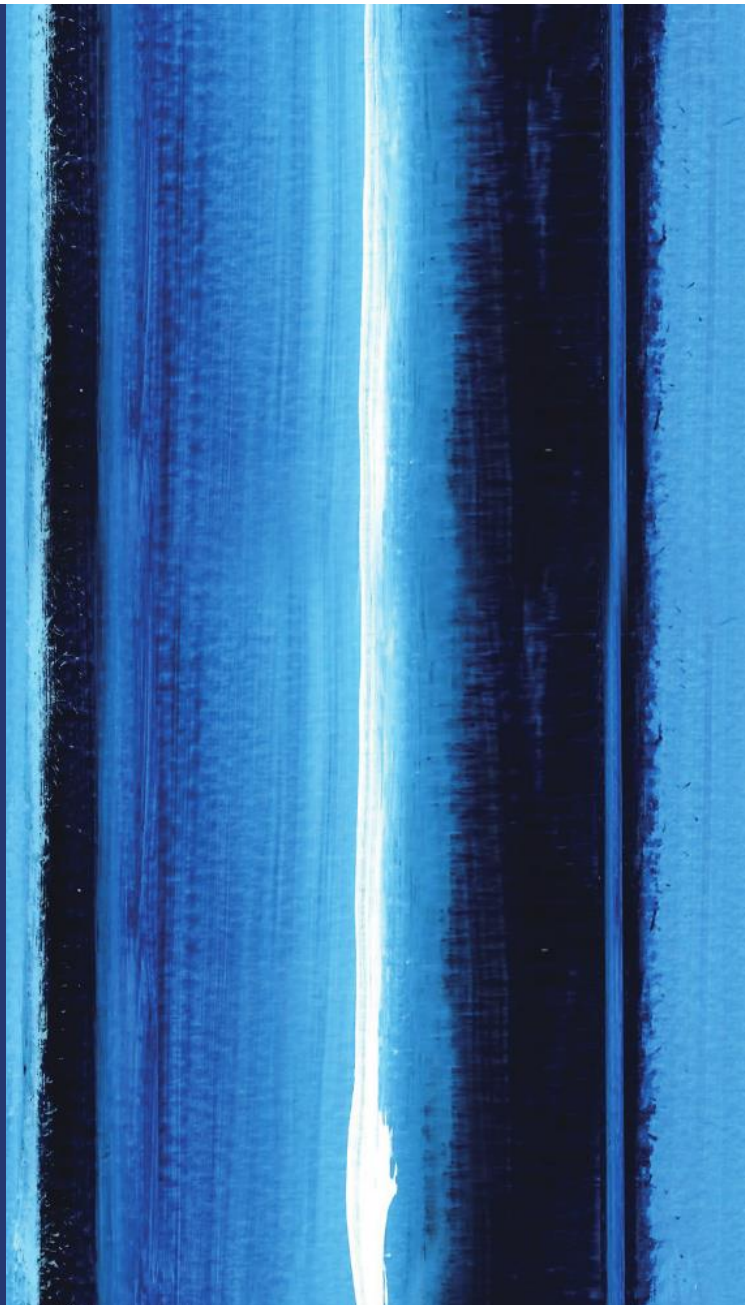
POUR LA SOLIDARITÉ
European think & do tank

LES DONNÉES PERSONNELLES

Le nouvel or noir aux multiples enjeux

Clara SERVEL et Alexis WILLEMOT

Sous la direction de
Denis STOKKINK



NOTES D'ANALYSE | JAN 20

Participation citoyenne

POUR LA SOLIDARITÉ
European think & do tank

COMPRENDRE POUR AGIR

LES DONNÉES PERSONNELLES
Le nouvel or noir aux multiples enjeux

Clara SERVEL et Alexis WILLEMOT
Sous la direction de Denis STOKKINK

SOMMAIRE

AVANT-PROPOS

Envoyer des mails, commander sur internet ou consulter les réseaux sociaux sont autant d'habitudes devenues quotidiennes qui nous obligent à laisser des traces, souvent à notre insu. Ces dernières, plus communément appelées « données personnelles » représentent aujourd'hui des ressources précieuses et stratégiques, souvent décrites comme le nouvel or noir du 21è siècle.

Très convoitées, ces données font face à une exploitation sauvage, accompagnée de nombreuses dérives. Ciblage publicitaire, hacking voire manipulation de l'opinion sont des pratiques devenues courantes. Ces dernières soulèvent des enjeux sécuritaires et démocratiques de premier plan. Face aux abus, les citoyen-ne-s européen-ne-s ont longtemps été impuissant-e-s, sans le moindre contrôle sur leurs données.

La protection des données répond ainsi à une double prérogative. À l'échelle individuelle, elle répond au respect des citoyen-ne-s et de leurs droits. À l'échelle globale, elle questionne l'intégrité démocratique et sécuritaire de nos sociétés contemporaines. Suite à sa précédente note d'analyse intitulée « Outils numériques, big data et citoyenneté », PLS a décidé de se saisir une nouvelle fois de cette thématique pour analyser à la fois les enjeux et menaces auxquelles sont exposées les données personnelles avant de s'interroger sur la pertinence des réponses proposées par l'Union Européenne.

Solidairement vôtre,

Denis Stokkink

INTRODUCTION

> ***« Ces règles innovantes ont […] permis à l'Europe de s'adapter à l'ère numérique. Leur objectif principal était de donner aux citoyen-ne-s le pouvoir d'agir et de les aider à mieux contrôler leurs données à caractère personnel. Or cet objectif est en cours de réalisation. »***
>
> – Andrus Ansip, vice-président pour le marché unique numérique

Entré en vigueur le 26 mai 2018, cela fait maintenant plus d'un an que le Règlement général sur la protection des données (RGPD) fait loi. Ce règlement est l'aboutissement de quatre années de négociations et d'un nombre record de 3999 amendements. Ce texte fut adopté par le Parlement européen le 14 avril 2016[1] pour répondre à deux objectifs principaux : harmoniser les règles concernant la protection des données personnelles au sein de l'Union Européenne et renforcer les standards de sécurité pour protéger à la fois les citoyen-ne-s et les entreprises.

Première mondiale, son édification illustre une prise de conscience croissante des enjeux relatifs aux données personnelles. En effet, ces thématiques liées aux nouvelles technologies et à l'informatique sont assez récentes et évoluent à un rythme très rapide. Le développement d'internet en est d'ailleurs un bon exemple. Ouvert au grand public dans les années 90, le réseau comptait déjà 47% d'utilisateur-rice-s européen-ne-s en 2005[2]. Un nombre qui n'a cessé de croitre depuis, pour atteindre les 80%[3] en 2018. Ainsi, en seulement deux décennies, Internet est passé d'une utilisation limitée par un public très restreint de spécialistes à un élément essentiel de la vie quotidienne. Or, face à cette évolution spectaculaire, l'Union européenne est restée pendant longtemps immobile avec pour seule règlementation un texte de 1995, du temps où Internet n'était qu'à ses balbutiements[4].

Dans ce contexte nouveau et changeant, la production de données a été démultipliée par des phénomènes successifs. Le premier, dit le « Web 2.0 », a provoqué une transformation profonde d'internet par une simplification du réseau. Grâce à cela, les utilisateur-rice-s ont pu se l'approprier et être eux/elles même créateur-rice-s de contenu (blog, compte sur une plateforme de partage, publications sur les réseaux sociaux…) et par conséquent émettre et partager plus de données. Le second, l'Internet des objets, est plus récent et se traduit par l'élargissement de la connexion à Internet de nombreux objets du quotidien tels que les smartphones mais également les téléviseurs, montres, thermostats, etc. Cette plus grande connectivité permet un contrôle plus précis sur les objets, mais est avant tout productrice de données, tant sur les objets concernés que sur leurs propriétaires.

Ces différentes transformations ont conféré aux données personnelles une importance capitale. À la fois ressources économiques et enjeux politiques, elles sont désormais au cœur des intérêts d'une multitude d'acteurs. La mise en application du RGPD, en mai 2018, témoigne d'une prise de conscience croissante de l'importance des données personnelles, tant par les États que par les citoyen-ne-s. Face à ce constat, POUR LA SOLIDARITÉ a voulu présenter brièvement les enjeux majeurs entourant ces données avant de se questionner sur la capacité du RGPD à assurer une protection effective de citoyen-ne-s après un an d'application.

[1] Parlement européen, « Q&R : Les nouvelles règles de l'UE sur la protection des données placent les citoyen-ne-s aux commandes », Background, 01/06/2016.
[2] Wikipédia, « Liste des pays nombre d'utilisateurs d'Internet », page mise à jour le 3/08/19.
[3] COEFFÉ Thomas, « Chiffres internet 2018 », *BDM Média*, 29/08/19.
[4] Parlement européen et Conseil européen « DIRECTIVE95/46/CE », 24/10/1995.

I. LES DONNÉES PERSONNELLES, UNE RESSOURCE ÉCONOMIQUE ET TECHNOLOGIQUE

1. LES DONNÉES AU CŒUR DE L'INTELLIGENCE ARTIFICIELLE

En même temps qu'Internet s'étend à toujours plus de domaines, notre production de données connaît une croissance en apparence sans limite. Ainsi, à chaque minute, la population mondiale envoie 473 000 tweets, écoute 750 000 morceaux sur Spotify et exécute 3 887 000 recherches sur le moteur de recherche Google[5]. En parallèle, l'intelligence artificielle connaît un essor spectaculaire depuis plusieurs années. Sous cette appellation couvrant un large spectre de technologies, une notion apparaît centrale : le Machine Learning (ou apprentissage automatique). En très résumé, il s'agit de machines capables d'apprendre par elles-mêmes des choses pour lesquelles elles n'ont pas été programmées. Elles peuvent alors reconnaître des chiens sur des images, déchiffrer des écritures manuscrites, traduire des textes, etc. En juillet 2017, DeepMind, une entreprise spécialisée dans l'intelligence artificielle appartenant à Google, a réalisé l'exploit d'élaborer un programme qui a appris par lui-même à marcher, courir, sauter et franchir des obstacles sur différents types de terrain. Pour ce faire, il lui a été donné comme consigne de se rendre d'un point A à un point B, sans aucune instruction sur la méthode à employer. Procédant par essai-erreur et intégrant les expériences passées dans ses algorithmes, le programme a rapidement réussi à « découvrir » la marche[6].

Les données ont un rôle central dans le développement de cette technologie qui requiert des volumes considérables. En effet, avant d'être suffisamment performante pour pouvoir réaliser les tâches souhaitées, la machine nécessite de passer par une phase d'entraînement durant laquelle elle « apprend » à partir d'exemples, c'est-à-dire qu'elle élabore des algorithmes efficaces à l'aide de grandes quantités de données qui lui sont fournies[7]. Ainsi, plus les données sont nombreuses, plus les algorithmes seront précis et efficaces. Prenons l'exemple des chiens[8]. Il a fallu disposer d'une banque d'images afin que peu à peu, le programme identifie des *patterns* permettant de distinguer les représentations de l'animal d'autres images. Détenant des quantités de données gigantesques, les GAFA (Google, Amazon, Facebook et Apple) sont les mieux placés pour le développement de cette technologie qui va sans aucun doute révolutionner notre monde, comme ont pu le faire la machine à vapeur, l'électricité, l'informatique ou Internet[9].

2. LES DONNÉES AU SERVICE DU MARKETING

Les données représentent également un grand intérêt économique en termes de publicité. Leur usage à des fins commerciales est une vraie révolution dans le secteur du marketing. Les stratégies traditionnelles visant à toucher le plus grand nombre ont été laissées de côté au profit de campagnes ciblées, sur base des données collectées. Il est important de souligner que ces outils marketing ont pu se développer grâce au flou législatif qui entourait l'utilisation des données jusqu'à l'entrée en vigueur du RGPD en mai 2018.

[5] COEFFÉ Thomas, « Chiffres Internet 2018 », *Le Blog du Modérateur*, 29/08/2018.
[6] Une vidéo présentant cet exploit est disponible en ligne : https://www.youtube.com/watch?v=gn4nRCC9TwQ
[7] Datatilsynet, *Artificial intelligence and privacy. Report January* 2018, 2018.
[8] LECUN Yann, BENGIO Yoshua, HINTON Geoffrey, « Deep learning », *Nature*, vol. 521, 28 mai 2015, pp. 436-444.
[9] ALEXANDRE Laurent, *La guerre des intelligences : intelligence artificielle versus intelligence humaine*, Paris : Jean-Claude Lattès, 2017.

Il est de plus en plus courant d'opérer par ciblage comportemental. Cela revient à proposer des publicités en accord avec les intérêts des utilisateur-rice-s tels qu'identifiés à l'aide des *cookies*. Ces derniers sont des fichiers qui enregistrent les recherches effectuées, les pages consultées, les produits mis en panier sur des sites d'achats en ligne, les clics sur bannières publicitaires, etc. En clair, les *cookies* collectent de données à propos d'un utilisateur. Le plus célèbre est AdWords de Google. Il repose sur le très large éventail des services proposés par la firme, notamment le contenu des mails échangés par Gmail. Néanmoins, plusieurs problèmes éthiques sont posés par cette technique, notamment la possibilité donnée à n'importe qui d'espionner les particuliers pour un coût extrêmement faible[10].

À présent, l'objectif des entreprises est de proposer la publicité la plus adéquate à ses client-e-s pour les satisfaire au mieux, ce qui a encouragé le développement de *l'Account-Based Marketing* (ABM)[11]. Contrairement aux campagnes publicitaires classiques qui visent à atteindre le plus grand nombre d'individus, l'ABM consiste à concentrer ses ressources sur un plus petit nombre de client-e-s potentiel-le-s ciblés en leur proposant des annonces personnalisées en accord avec leurs intérêts. La publicité se place ainsi au niveau de l'individu et non plus du groupe. Cette stratégie permettrait d'augmenter la satisfaction du client de 30 à 50%[12]. Même si cette technique nécessite la capacité de traiter un grand nombre de données personnelles pour être vraiment efficace elle marque sans nul doute une véritable adaptation du marketing face à la prolifération des données.

Cette course à l'innovation marketing semble sans limite et d'autres entreprises encore vont plus loin grâce à la méthode du *Real-time creative* (RTC)[13]. À partir des données collectées, des micros bassins d'influence vont être identifiés pour créer des publicités distinctes et adaptées à chacun d'eux. L'objectif est d'optimiser l'attractivité de la publicité et d'élargir le public concerné tout en restant au plus près des intérêts de l'utilisateur. Le cas de Legendary Entertainment et de sa stratégie mise en place pour la sortie du film Warcraft (2016) est un bon exemple du succès de cette méthode. À partir des différentes thématiques du film, la firme a identifié plusieurs bassins d'influences et fait une bande annonce pour chacun d'entre eux. Grâce à ça, les bandes annonces ont comptabilisé plus de 100 millions de vues en à peine une semaine. Il ne faut pas pour autant perdre de vue que ces outils marketing ne sont que des moyens, l'objectif final étant de générer des mannes financières toujours plus élevées.

3. UN SECTEUR LUCRATIF

En raison des ressources que les données représentent à l'égard de ces deux domaines, une véritable industrie se développe. Pour 2019, le marché mondial de la publicité en ligne est estimé à 200 milliards de dollars[14]. De son côté, le chiffre d'affaire mondial produit par le Big Data (ou données massives) s'élevait à 56 milliards de dollars en 2017 avec une prévision de 210 milliards de dollars prévue en 2020. Un secteur porteur puisqu'il devrait peser pour 3% dans la croissance du PIB de l'Union européenne en 2020[15]. Or, comme le résume assez bien le slogan *« si c'est gratuit, c'est que vous êtes le produit »*, le fonctionnement de ces services gratuits nécessite des rentrées financières, obtenues grâce à la revente des données personnelles qui permettent à ces entreprises d'engranger des bénéfices colossaux.

Ce segment compte également les *data brokers*, des courtiers qui achètent et revendent les données. Ainsi, le géant Acxiom tire des millions de revenu grâce aux 1500 informations en moyenne qu'il possède sur plus de 200 millions de citoyen-ne-s américain-e-s pour une population de 331 millions[16]. Notons qu'il existe à ce niveau une grande différence entre les États-Unis et l'Europe, cette dernière s'intéressant

[10] VINES Paul, ROESNER Franziska, KOHNO Tadayoshi, « Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob », 16e ACM Workshop on Privacy in the Electronic Society, 30/10/2017.
[11] ROSE Michael, « What Is Account-Based Marketing? », *Forbes Community Voice*, 01/11/2017.
[12] Institut de l'Internet et du multimédia, La « data révolution » dans le marketing digital , 28/10/16.
[13] Institut de l'Internet et du multimédia, La « data révolution » dans le marketing digital , 28/10/16.
[14] GODARD Bruno, « Comment les publicitaires suivent vos traces sur le Net grâce aux cookies », *Capital*, 29/08/2019.
[15] Corp, « L'Infographie officielle du Big Data en 10 chiffres clés », 28/02/2019.
[16] États-Unis, *Data Population*, le 29/08/2019.

plus à la protection des données personnelles comme en témoigne l'entrée en vigueur du Règlement général sur la Protection des Données (RGPD) en mai 2018. En même temps que l'Union se mettait d'accord sur le nouveau règlement, le Sénat américain autorisait les fournisseurs d'accès à Internet à vendre les données personnelles de leurs clients sans que leur consentement soit requis.

Des sommes faramineuses sont amassées grâce aux données que les utilisateur-rice-s offrent aux plateformes, sans que ces dernier-ère-s ne soient rémunéré-e-s pour leur création de valeur ni qu'iels aient accès à ces données. Le think thank français Génération Libre en parle comme d'une « dépossession » et propose de rendre l'individu à nouveau propriétaire de ses données en lui offrant la possibilité de les vendre aux entreprises du numérique[17]. Bien que la proposition soit controversée, elle souligne la nécessité croissante de s'intéresser à l'enjeu des données personnelles, de leur utilisation et de la répartition des revenus qui en sont tirés.

[17] Génération Libre*, Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018.

II. L'EXPLOITATION DES DONNÉES, UNE MENACE INÉDITE POUR NOS SOCIÉTÉS CONTEMPORAINES

1. DES CYBERATTAQUES EN CONSTANTE AUGMENTATION

Les cyberattaques ne sont pas un phénomène nouveau. Bien que concomitantes au développement de l'informatique[18], elles ont connu une croissance considérable avec l'apparition et le développement d'Internet. En effet, l'expansion fulgurante du réseau et son immixtion dans toujours plus de domaines de la vie privée et professionnelle les a rendus vulnérables aux attaques. À cet égard, L'Agence nationale de la Sécurité des Systèmes d'Information française (ANSII) publie un rapport annuel dans lequel elle identifie les grandes tendances en matière de menaces[19]. En 2018, elle a recensé notamment l'exfiltration de données stratégiques, les attaques indirectes et les opérations de déstabilisation et d'influence. Ces menaces sont d'autant plus difficiles à combattre qu'elles évoluent très rapidement comme l'illustre son rapport de 2017[20]. Aussi, si certaines tendances semblent se confirmer telles que les attaques indirectes, d'autres ont déjà mutées. C'est le cas des attaques massives non ciblées qui ont beaucoup frappées en 2017 mais qui ont disparues en 2018 suite à la hausse des systèmes de sécurité. D'autres méthodes, plus adaptées au nouvel environnement numérique ont vu le jour pour les remplacer. Face à ces attaques, même les plus grandes firmes du secteur technologique sont menacées, comme en témoigne la récente fuite de données dont fut victime Facebook en avril 2019. Près de 540 millions d'utilisateur-rice-s se sont vus dérober des informations les concernant à partir d'une faille dans le système de sécurité d'une application tierce, sur laquelle les utilisateur-rice-s s'inscrivaient à partir de leur profil Facebook[21]. C'est la plus grande fuite de données jamais enregistrée mais son cas n'est pas isolé, à l'image d'Uber qui s'était fait voler les données de 57 millions d'utilisateur-rice-s et 600 000 chauffeurs. L'enjeu est de taille puisque ces informations peuvent ensuite être réutilisées à des fins illicites, et plus particulièrement en matière d'usurpation d'identité[22].

L'enjeu de la cybersécurité est d'autant plus élevé que les cyberattaques prennent différentes formes, répondent à différents objectifs. Le cas des *ransomwares* en est un exemple frappant. Traduit en français sous le terme de « rançonlogiciel », c'est un logiciel malveillant qui crypte les fichiers des ordinateurs infectés et exige ensuite une rançon pour en récupérer l'accès (sans certitude de l'obtenir une fois le paiement exécuté). En mai 2017, la plus grande cyberattaque du genre est lancée au moyen du logiciel WannaCry[23]. Ce dernier infecta plus de 300 000 ordinateurs répartis dans 150 pays en exploitant une faille de Windows, pourtant corrigée par une mise à jour parue en mars de la même année. Négligée par de nombreux particuliers et entreprises, cette faille n'a pas été refermée, permettant ainsi au virus de se répandre lorsque les règles de sécurité élémentaires comme celle de ne pas ouvrir d'e-mail d'origine inconnue n'étaient pas respectées[24]. La faille a d'abord été découverte et exploitée par la National Security Agency (NSA) avant d'être révélée au grand jour par le groupe de hackers « The Shadow Brockers » suite au piratage de documents confidentiels de la NSA.

[18] BAUMARD Philippe, « The behavioral paradigm shift in fighting cybercrime: Counter-measures, innovation and regulation issues », *International Journal on Criminology*, 2(1), 2014, pp.11-22.
[19] L'Agence Nationale de Sécurité de l'Information, *Rapport annuel 2018*, 2018.
[20] L'Agence Nationale de Sécurité de l'Information , *Rapport d'activité 2017*, 2017.
[21] « Facebook victime d'une nouvelle fuite de données: 540 millions d'utilisateurs concernés », *la RTBF*, le 04/04/2019
[22] L. Bastien, « Uber a caché la fuite de données personnelles de 57 millions d'utilisateurs et de chauffeurs », *Le Big Data*, 23/11/2017.
[23] GRAHAM Chris, « NHS cyber attacks: Everything you need to know about the 'biggest ransomware' offensive in history », *The Telegraph*, 20/05/2017.
[24] ZAFFAGNI Marc, « Cyberattaque WannaCry : 98% des PC touchés par le ransomware étaient sous Windows 7 », *Futura*, 22/05/2017.

Parmi les victimes, on compte le National Health Service (le service de santé britannique) dont le piratage entraîna la paralysie des systèmes informatiques de 45 hôpitaux et empêcha l'accès aux dossiers des patients. Un mois après WannaCry, un second logiciel est apparu le 27 juin 2017. Nommé NotPetya, il exploita la même faille et toucha notamment plusieurs banques en Ukraine ou encore la centrale nucléaire de Tchernobyl. Les attaques, bien que de moins grande ampleur, restent récurrentes comme en atteste l'une des dernières attaques en date, qui a paralysé l'ensemble du réseau informatique des services publics de l'état du Texas[25].

Au-delà de la cybercriminalité, ces dernières années ont vu la « cyberguerre » gagner en ampleur. En effet, de plus en plus de secteurs de première importance pour les pays et populations fonctionnent grâce à Internet, faisant de ce dernier un lieu de confrontation militaire majeur entre les États (favorisé également par la difficulté d'identification de l'origine des attaques). À ce niveau, les pays les plus développés sont également les plus vulnérables en raison de la place importante qu'occupent leurs infrastructures numériques, créant par-là une véritable dépendance aux technologies de l'information[26]. Or, beaucoup de ces pays ont mis l'accent sur leur développement économique à travers la numérisation rapide, et au détriment de leur sécurité numérique[27]. Ils se révèlent dès lors plus vulnérables face aux attaques qui permettent aux assaillants de dérober des données ou de déstabiliser un pays. Ce type de confrontation a pris énormément d'ampleur durant ces dernières années et est indéniablement appelé à poursuivre sa croissance dans les décennies à venir. On pourrait citer un exemple survenu en avril 2018 : les États-Unis et le Royaume-Uni ont accusé la Russie[28] d'être à l'origine du piratage de millions d'appareils à travers le monde, notamment des appareils domestiques[29]. Les objectifs poursuivis relèveraient ainsi de l'espionnage, du vol de propriétés intellectuelles ou du positionnement pour une utilisation en période de tension.

Le développement de l'Internet des objets a également contribué à étendre la menace. Il est défini par l'Union internationale des télécommunications comme une *« infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution »*[30]. Autrement dit, cela consiste à implanter le partage de données via Internet, Bluetooth ou tout autre système à un nombre croissant d'objets de la vie quotidienne (ex : voitures autonomes ou non, éclairages, thermostats, caméras, et même pots de fleurs) afin de récolter et traiter les données. Cependant, ces objets connectés révèlent bien souvent de grandes lacunes sécuritaires. Selon une étude menée par Test Achats sur 19 appareils intelligents, cinq jours furent suffisant à deux hackers pour en pirater la moitié[31]. Parmi eux, on peut citer le piratage d'un thermostat permettant de le contrôler à distance et d'obtenir les données afin de savoir quand sont absents les habitants, ou encore celui d'une tablette pour enfants qui offre la possibilité d'écouter les utilisateurs, obtenir les images prises ou encore d'envoyer des contenus dessus.

Ainsi, face à la multiplicité et la croissance des attaques, toutes les strates de la société semblent vulnérables. Ce n'est plus seulement les personnes de manière individuelle qui sont menacées mais bien l'espace public en général. À cela s'agrège une nouvelle source d'inquiétude : l'instrumentalisation possible des données volées à des fins illicites voire anti-démocratiques.

[25] FERNANDEZ Manny, ZAVERY Mihir et S. RUEB Emily « Ransomware Attack Hits 22 Texas Towns, Authorities Say », *The New York Times*, 20/08/19.
[26] LUIGGI Jean-Sun, « Cyberguerre, nouveau visage de la guerre ? », *Stratégique*, vol. 112, n°2, 2016, p.91-100.
[27] Rapid7, National Exposure Index. *Inferring internet security posture by country through port scanning*, 2017.
[28] DEARDEN Lizzie, « Russian hackers targeting millions of devices around the world, US and UK warn », *Independent*, 16/04/2018.
[29] US-CERT, Alert (TA18-106A) : *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*, 16/04/2018 (mis à jour le 20/04/2018).
[30] Union internationale des télécommunications, « Série Y : Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaines génération. Réseaux de prochaines génération – Cadre général et modèles architecturaux fonctionnels. Présentation générale de l'Internet des objets », *Secteur de la normalisation des télécommunications de l'UIT*, 2012, p.1.
[31] BOSSELER Julien, « Nos objets connectés, mine d'or pour les hackers », *Le Soir*, 03/05/2018, p.18.

2. LA MISE EN PÉRIL DU PROCESSUS DÉMOCRATIQUE

En 2018, l'affaire de Cambridge Analytica (CA) a défrayé la chronique en révélant l'utilisation malveillante de données personnelles pour orienter les élections. Le 17 mars 2018, le *New York Times*[32] et *The Guardian*[33] ont révélé l'implication de la firme dans plusieurs scrutins électoraux, dont ceux qui ont vu triompher Donald Trump aux États-Unis et le Brexit au Royaume-Uni. Le lanceur d'alerte est Christopher Wylie, l'un des fondateurs de CA et employé jusque fin 2014. Il a exposé au grand jour les méthodes de l'entreprise qui collectait un maximum de données – légalement et illégalement – pour ensuite les utiliser dans le but de manipuler les élections en faveur de leurs client-e-s. Parmi ces dernier-e-s, on retrouve l'équipe de Donald Trump et celle du « leave » (pro-brexit), mais aussi des ministères de la Défense de plusieurs pays ainsi que des militaires. Pour satisfaire ses client-e-s, l'entreprise proposait divers services tels que la collecte privée de renseignements et d'informations pouvant compromettre une opposition, la création de rumeurs, la diffusion de *fake news* pour renforcer *l'alt-right*, la mise en place de pièges...[34] Pour ce faire, elle a exploité une faille de Facebook permettant d'obtenir des informations sur 87 millions d'utilisateur-rice-s du réseau social[35] grâce à un quiz proposé contre rémunération. Le géant de la Silicon Valley s'est alors trouvé dans la tourmente pour ne pas avoir pris les mesures nécessaires garantissant la protection des données de ses utilisateur-rice-s. De plus, l'affaire a démontré l'usage potentiellement détourné qui peut être fait des données, interrogeant ainsi l'essence même de l'activité de Facebook[36].

Ce scandale expose le poids des données numériques, et des firmes qui les possèdent, dans le processus politique et soulève de nombreuses questions quant à leurs effets sur la démocratie. Bien qu'il soit difficile de mesurer l'impact d'une campagne telle que menée par CA sur le résultat des élections, elle n'en demeure pas moins influente. Aussi, Christopher Wylie en parle comme relevant de la fraude électorale[37] et affirme que *« sans Cambridge Analytica, il n'y aurait pas eu de Brexit*[38] *»* ; le « leave » a emporté le référendum avec seulement 3,8% de voix supplémentaires[39]. Bien que des entreprises comme Google et Facebook n'utilisent pas les données dans l'intention d'en faire un usage néfaste, elles ont néanmoins acquis un poids qui leur confère une influence extraordinaire. Le sociologue Sami Coll explique ainsi que *« la multiplication des données donne un pouvoir considérable à des acteurs principalement issus des milieux économiques, ce qui met en péril une certaine vision de la démocratie et de l'organisation de la société »*[40].

Au-delà du vol de données à des fins politiques, le fait que les algorithmes organisent eux-mêmes une sélection des informations interroge sur leur capacité à nous influencer, orientant nos choix de manière insidieuse. C'est Eli Pariser qui a évoqué en premier cette possibilité, lors d'une conférence TED en 2011[41]. Parti du constat qu'il ne voyait plus les post Facebook de ses amis conservateurs, lui-même affilié aux démocrates, il s'est interrogé sur le possible rôle des algorithmes du média social dans la sélection du contenu proposé. En effet, les géants du net les ont progressivement développés afin de proposer le contenu jugé le plus adéquat pour l'utilisateur-rice, en fonction de ses centres d'intérêts établis grâce à ses navigations précédentes et aux publications de ses ami-e-s. Afin d'étayer sa théorie, il a demandé à deux amis à lui de taper « Égypte » sur internet. Alors que l'un avait des résultats concernant la situation géopolitique du pays, l'autre avait des sites de voyage. C'est une méthode qui peut paraître anodine au premier abord, mais qui pose en fait des questions démocratiques plus vastes concernant l'accès à l'information. Cet effet dit de *bubble filter* (bulle de filtre en français) nous enferme

[32] ROSENBERG Matthew, CONFESSORE Nicholas, CADWALLADR Carole, « How Trump Consultants Exploited the Facebook Data of Millions », *The New York Times*, 17/03/2018.
[33] CADWALLADR Carole, GRAHAM-HARRISSON Emma, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *The Guardian*, 17/03/2018.
[34] DELESALLE-STOLPER Sonia, « "Sans Cambridge Analytica, il n'y aurait pas eu de Brexit" », *Libération*, 26/03/2018.
[35] ALIX Christophe, « Facebook pris dans la tempête de l'affaire Cambridge Analytica », *Libération*, 20/03/2018.
[36] CHERIF Anaïs, « Cambridge Analytica : Facebook au cœur d'un nouveau scandale », *La Tribune*, 20/03/2018.
[37] SCOTT Mark, « Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower », *Politico*, 27/03/2018 (mis à jour le 29/03/2018).
[38] DELASALLE-STOPER, « "Sans Cambridge Analytica, il n'y aurait pas eu de Brexit" », *Libération*, 26/03/2018.
[39] The Electoral Commission, « EU referendum results ».
[40] FARINE Mathilde, « "La multiplication des données met en péril une vision de la démocratie" », *Le Temps*, 22/05/2017.
[41] TED vidéo "Eli Pariser beware online filter bubbles" disponible ici : https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=fr

dans une bulle dans laquelle *« internet nous montre ce qu'il pense que nous voulons voir, pas ce que nous avons besoin de voir »* [42] selon Eli Pariser et opère ainsi un filtrage subjectif de l'information. L'algorithme masque les contenus qui portent des opinions différentes/opposées aux vôtres ou dont les thématiques ne rentrent pas dans vos centres d'intérêts déjà identifiés. Pour le politologue Patrick Troude-Chastenet ces pratiques reviennent à organiser « une propagande univoque » [43]. Il poursuit la réflexion en alertant sur un autre danger lié à ces bulles, la possible propagation de *fake news* sans autre source d'information pour la contrebalancer. L'intérêt d'une *fake news* repose sur sa capacité à se propager. Pour parvenir à toucher le plus grand nombre les hackeurs utilisent des bots, intelligences artificielles capables de reproduire les comportements humains, qui pourront simuler une fausse vague de popularité sur le média social et ainsi diffuser le contenu un maximum. Par le système de filter bubble, il suffira qu'un seul de vos amis lise/like/partage la *fake news* pour quelle arrive jusqu'à vous. Ces bulles seraient donc un accélérateur de *fake news*. C'est un constat d'autant plus préoccupant dans un contexte de montée des populismes, encouragés par les *fake news* et la défiance vis-à-vis des médias traditionnels. Notons tout de même que les théories concernant l'existence de telles bulles sont contestées, bien que le fonctionnement des algorithmes soit lui bien réel.

Alors que l'influence des GAFA sur nos sociétés est considérable, la façon dont les entreprises collectent, traitent et utilisent les données reste opaque en raison du secret industriel. Les dirigeant-e-s de ses compagnies ne sont pas non plus élu-e-s et n'ont aucun compte à rendre aux citoyen-ne-s. Face au constat que *« l'entreprise est une entité politique »*[44], des voix s'élèvent, dont celle de la sociologue Isabelle Ferreras[45], afin d'instaurer une gouvernance démocratique au sein des compagnies[46]. Que l'on juge l'idée bonne ou non, elle a au moins le mérite de poser la question de l'adaptation de nos sociétés aux nouvelles technologies et moyens de production.

[42] TED vidéo "Eli Pariser beware online filter bubbles" disponible ici : https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=fr
[43] Patrick Troude-Chastenet, « Fake news et post-vérité. De l'extension de la propagande au Royaume-Uni, aux États-Unis et en France", *Quaderni n°96*, Février 2018
[44] FARINE Mathilde, "La multiplication des données met en péril une vision de la démocratie" , *Le Temps*, 22/05/2017.
[45] FERRERAS Isabelle, « "Il faut faire bénéficier les entreprises françaises d'un choc de compétitivité démocratique" », *Le Monde*, 19/04/2018 (mis à jour le 20/04/2018).
[46] FERRERAS Isabelle, *Firms as Political Entities, Saving Democracy Through Economic Bicameralism*, Cambridge : Cambridge University Press, 2017.

III. LE RGPD, UNE PROTECTION EFFICACE POUR LES DONNÉES PERSONNELLES ?

1. UNE QUÊTE D'ÉQUILIBRE ENTRE PROTECTION DES DONNÉES ET DYNAMIQUES ÉCONOMIQUES

Afin d'enrayer les dérives liées aux multiples utilisations des données personnelles, l'Union européenne a édicté un règlement général sur la protection des données (RGPD) en avril 2016[47]. Cette nouvelle norme juridique fait figure de pionnière au niveau mondial mais n'est pourtant pas la première réglementation adoptée par l'Union européenne en matière de protection[48]. Par une directive 95/46/CE, la Commission avait déjà fixé des conditions à l'utilisation des données. Cependant, bien vite rattrapées par la montée du numérique, ces normes sont rapidement devenues obsolètes et ont conduit à une fragmentation des législations nationales. Face à ce manque d'uniformité en matière de contrôle des données, l'UE a décidé d'agir.

La première visée de ce texte est de garantir et renforcer les libertés et droits fondamentaux des personnes physiques en matière de protection des données personnelles. Une obligation qui est d'ailleurs inscrite dans la Charte des droits de l'UE[49]. Afin de garantir une protection effective aux citoyen-ne-s de l'Union européenne, de nouveaux droits leur ont été reconnus :

DROIT À L'INFORMATION	Lorsque qu'un service informatique collecte des données sur un individu, il doit lui transmettre des informations telles que son identité, les finalités de sa collecte ainsi que les destinataires.
DROIT À LA RECTIFICATION	Une personne a le droit, à tout moment, d'obtenir la rectification de données inexactes sur sa personne.
DROIT D'ACCÈS AUX DONNÉES PERSONNELLES	Une personne peut, à tout moment, exiger d'une entreprise qu'elle lui transmette l'ensemble des données collectées à son sujet.
DROIT À LA RECTIFICATION	Si les données collectées sur une personne s'avèrent inexactes, cette dernière peut exiger une modification immédiate.
DROIT À L'OUBLI	Une personne peut exiger l'effacement des données collectées. L'entreprise doit alors prendre les mesures nécessaires, et ce même si les données ont été rendues publiques.

[47] Parlement européen et Conseil, Règlement 2016/679, *Journal officiel de l'Union européenne*, 27/04/2016.
[48] Parlement européen et le Conseil, Directive 95/46/CE, 24/04/1995.
[49] Charte des droits fondamentaux de l'Union Européenne, *Journal Officiel des communautés européennes*, 18/12/2000.

DROIT À LA PORTABILITÉ DES DONNÉES	Les données peuvent être transmises d'une base de données à une autre de manière automatisée.
DROIT À LA LIMITATION DU TRAITEMENT	Cette requête est possible en cas de rupture du contrat de consentement, d'obtention illégale des données, si l'entreprise de collecte n'a plus usage de ces données ou si la personne s'est opposée à l'exploitation des données.
DROIT D'OPPOSITION	Toute personne, en fonction de sa situation particulière, peut exprimer son refus de l'exploitation de ses données, bien qu'elle soit fondée sur l'intérêt général ou l'intérêt légitime de l'entreprise.
DROIT D'OPPOSITION À UNE PRISE DE DECISION AUTOMATISÉE	Une personne a le droit de s'opposer à toute décision automatisée qui pourrait avoir des effets juridiques sur elle. Cela englobe notamment les méthodes de profilage marketing.

D'autre part le RGPD fixe aussi des obligations à respecter en matière d'exploitation des données qui viennent compléter les nouveaux droits. Toute structure collectant des données devra s'y plier. L'objectif est d'unifier les différentes règlementations nationales et soumettre toutes les entreprises européennes à un même degré de contrainte. À présent, les entreprises doivent respecter un panel de normes allant de l'obligation du consentement avant toute collecte de données à la limitation de la collecte des données personnelles à des finalités « déterminées, explicites et légitimes »[50]. Autre nouveauté, les exploitants se voient reconnaître une responsabilité en matière de traitement des données qui, en cas de non-respect des normes, les exposeraient à des amendes pouvant aller de 10 à 20 millions d'euros ou de 2% à 4% du chiffre d'affaires s'il s'agit d'une entreprise.

Au-delà des nouvelles obligations qu'impose le RGPD, l'enjeu de l'harmonisation règlementaire est tout autant juridique qu'économique. Par le biais de ces nouvelles règles communes, l'UE veut mener une action combinée afin de stimuler l'activité du secteur de l'économie numérique. Une règlementation européenne unique devrait ainsi permettre de réduire les coûts administratifs qu'engendraient les législations nationales distinctes et ainsi fluidifier le trafic[51] de données personnelles. Pour sa part, l'encadrement de l'exploitation des données vise aussi à redonner confiance aux citoyen-ne-s européens de manière à ce qu'ils soient rassurés, et transmettent plus facilement leurs données du marché numérique.

« Grâce à ces nouvelles règles, les citoyen-ne-s pourront avoir confiance quant à la manière dont leurs données sont utilisées, tandis que l'UE pourra pleinement profiter des possibilités offertes par l'économie fondée sur les données ».

– Andrus Ansip, vice-président pour le marché unique numérique

[50] Parlement européen et Conseil Européen, Règlement 2016/679, *Journal officiel de l'Union Européenne*, 27/04/2016.
[51] DECHAMPS Frédéric, DE CLERCQ CHOLÉ, « Tout ce que vous devez savoir sur le RGPD », *Qualifio*, 2018.

2. UN CONSTAT MITIGÉ APRÈS UN AN D'APPLICATION

1.1. UN DISPOSITIF JURIDIQUE ET REPRESSIF INÉDIT

Cela fait maintenant plus d'un an que le RGPD est appliqué au sein de l'Union européenne et les changements opérés sont notables, voire encourageants pour certain-e-s. C'est en tout cas l'avis d'Andrus Ansip, ex-vice-président pour le marché unique numérique, et Věra Jourová, ex-commissaire pour la justice, les consommateurs et l'égalité des genres, déclarant : *« L'objectif principal était de donner aux citoyen-ne-s le pouvoir d'agir et de les aider à mieux contrôler leurs données à caractère personnel. Or cet objectif est en cours de réalisation »*[52]. À leurs yeux, la réussite du RGPD repose notamment sur la sensibilisation des citoyen-ne-s quant à leurs nouveaux droits. En effet, en 2019, près de 73% des européen-ne-s connaissaient au moins l'un de leurs 9 droits et 57% étaient au courant de la mise en application du RGPD[53] et près de 145 000 plaintes avaient été enregistrées auprès des autorités de protections des données. Des chiffres positifs qui démontrent une prise de conscience de la part des citoyen-ne-s de l'UE de leurs droits et la possibilité de les faire valoir devant une autorité compétente. Pour autant, ces avancées restent fragiles puisque, seuls 20%[54] d'entre elles-eux pourraient nommer leur agence nationale de protection des données.

Malgré ces chiffres, le rôle des agences nationales de protection des données s'est pourtant accru, permettant enfin d'instaurer un réel contrôle de l'exploitation des données. Il n'y avait jusque-là aucune obligation pour un pays à détenir une entité de contrôle et leur gestion était entièrement libre. Cela provoquait des inégalités en matière de protection entre les pays et les actions des agences nationales étaient disparates et isolées. Aussi, l'une des avancées du RGPD est d'avoir créé un comité européen de protection des données. Ce dernier vise à coordonner les actions entre les agences nationales et leur mettre de nouveaux outils à disposition. Grâce à lui, les agences nationales ont vu leurs capacités renforcées. Encouragée par cette nouvelle dynamique, la première sanction n'a pas tardé à tomber, en octobre 2018, lorsque la commission nationale de protection des données portugaise a condamné un hôpital à hauteur de 400 000 euros pour manquement au RGPD. L'hôpital avait délivré près de 950 habilitations à des médecins, leur permettant alors d'avoir accès aux informations médicales et personnelles des patients, quand moins de 300 d'entre eux travaillaient réellement dans l'établissement[55]. Un accès d'autant plus alarmant, compte tenu du nombre de données sensibles détenues par un hôpital. Cependant, si la première structure épinglée était publique, les agences de protections des données enquêtent principalement sur les GAFA au vu du nombre de plaintes déposées à leur encontre. À ce titre, en février 2019, l'Office fédéral allemand de lutte contre les cartels a condamné Facebook pour non-respect du RGPD dans la collecte des données et abus de position dominante. La firme multinationale avait en effet recours à un stratagème : les conditions d'utilisation de Facebook incluaient la collecte de données dans ses succursales (Instagram, Messenger et WhatsApp) et sur tous les sites tiers comportant des mentions « j'aime », détournant ainsi l'obligation de consentement[56].

Malgré leurs sanctions, ces autorités rencontrent cependant des limites, contenues elles-mêmes dans le RGPD qui fixe la primauté à l'autorité du pays dans lequel se trouve le siège social de l'entreprise[57]. Dans le cas des GAFA c'est l'Irlande qui fait autorité, et ce malgré que leur autorité nationale soit encore en construction et disposant, jusque-là, de très faibles moyens financiers. Une faille que les géants du numériques tentent d'exploiter afin d'échapper aux sanctions, à l'image de Google qui a fait appel face à la condamnation de la CNIL (France) en janvier dernier en exigeant d'être rejugé en Irlande cette fois. Néanmoins, ce bras de fer n'est pas près d'être gagné par les GAFA au vu des déclarations de Helen

[52] Commission européenne, « Règlement général sur la protection des données: bilan de la première année », 22/05/2019.
[53] Commission européenne, « Le règlement général sur la protection des données donne des résultats, mais les travaux doivent se poursuivre », 24/07/19.
[54] LAZZAROVICI Marianne, « RGPD : quel bilan un an après sa mise en œuvre ? », *Toute l'Europe*, 8/08/19.
[55] CHEMINAT Jacques, « Première amende RGPD pour un hôpital portugais », *CIO*, 5/11/2018.
[56] DELEPINE Justin, « Paris s'attaque à Google et Berlin à Facebook », *Alternatives Économiques*, 1/03/19.
[57] HERRERO Océane, « RGPD: l'Irlande assignée gendarme de l'Union européenne », *l'Opinion*, 19/02/19.

Dixon, nouvelle directrice de la Data Protection Commission (Irlande), affirmant que la condamnation de Google par la CNIL ne serait *« pas la dernière »*[58].

1.2. DES LIMITES JURIDIQUES ET TECHNOLOGIQUES

Bien que le RGPD représente une avancée inédite en matière de protection des données personnelles, ses limites tant juridiques que technologiques sont déjà visibles. Très vite, le nouveau règlement a été mis face à ses contradictions et alors même que le RGPD a pour objectif de sécuriser les données, il rendrait leur vol d'autant plus accessible. C'est ce que pointent en tout cas les recherches de James Pavur, spécialiste en cybersécurité[59]. Il a mis en évidence que le droit conféré aux citoyen-ne-s « d'accès à leurs données personnelles » n'était pas assorti des garanties de sécurité nécessaires. Pour cela, il s'est fait passer pour sa petite amie auprès de 150 entreprises en leur réclamant l'ensemble des données en leur possession sur elle. Sur l'ensemble des réponses obtenues, 108 au total, 25% n'ont exigé aucun contrôle d'identité et seulement 39% ont demandé un justificatif considéré d'un niveau correct. Grâce à cela, le chercheur a réussi à amasser près de 60 types de données différentes sur sa petite amie dont certaines considérées comme « sensibles » telles que l'adresse, le numéro de sécurité sociale ou encore le numéro de carte bancaire. Cette faille en matière de sécurité provient d'un flou juridique contenu dans le règlement qui laisse les précautions en matière de contrôle d'identité à la libre appréciation du responsable du traitement des données. Ce manque de protection est donc imputable à des standards juridiques trop faibles de protection, accentué par des inégalités de moyens. En effet, en affinant son étude James Pavur a démontré que les données les plus faciles à dérober étaient celles transmises par les PME. Face aux coûts exorbitants du RGPD, nombre d'entre elles ont appliqué le règlement *a minima* et n'ont pas débloqué de fonds supplémentaires afin de garantir une sécurité effective. Aussi, cette situation provoque un risque inégal, inconnu et légal pour l'utilisateur qui ne peut savoir si la plateforme à qui il confie ses données à les moyens de véritablement les protéger.

Par ailleurs, la compétence du RGPD est menacée par l'innovation technologique. Alors que ses principes juridiques sont figés dans le règlement, le numérique est lui en constante évolution. Cela accroît par conséquent le risque de l'émergence de nouveaux outils digitaux hors de l'encadrement prévu par le RGPD. Si cette hypothèse peut paraître abstraite et lointaine elle est en réalité déjà effective. La « ré-identification » des données personnelles en est d'ailleurs la preuve. Selon l'article 9 du règlement, la vente de toute donnée dite « sensible » est interdite. Cette catégorie comprend notamment les origines ethniques, les croyances religieuses, l'orientation sexuelle, les données biométriques ou encore le passé médical. Afin de détourner cette interdiction et pouvoir exploiter les données, les entreprises publiques comme privées ont recourt à un processus dit « d'anonymisation ». En taisant le nom du propriétaire de ces données, ces dernières perdent leur caractère « personnel » et ne sont donc plus soumises à la règlementation du RGPD. Une faille juridique loin d'être sans conséquence comme l'a démontré une étude rendue publique le 23 juillet 2019 menée par des chercheurs de l'Université catholique de Louvain et de l'Imperial College of London[60]. À partir d'un algorithme, ils ont réussi à identifier formellement une personne dans une base de données censée être anonyme. Pour cela, les chercheurs ont programmé le logiciel à séquencer les données récoltées pour progressivement individualiser les profils de la manière suivante : *« [si] beaucoup de personnes vivant à New York sont des hommes et ont la trentaine. Parmi elles, beaucoup moins sont également nées le 5 janvier, conduisent une voiture de sport rouge, ont deux enfants (des filles) et un chien »*[61]. Dans 99,98% des cas il ne faut que 15 informations sur une personne pour la retrouver. À partir de là, toutes les données personnelles récoltées sont accessibles et exploitables sans aucun contrôle. Cette étude, qui n'est qu'une illustration, apporte ainsi la preuve que le développement d'un logiciel assez puissant est capable de contourner des normes juridiques qui n'ont pas, et ne peuvent pas prévoir l'émergence de futures technologies.

[58] HERRERO Océane, « RGPD: l'Irlande assignée gendarme de l'Union européenne », *l'Opinion*, 19/02/19.
[59] GALLENBORN Gilbert, « Paradoxalement, le RGPD facilite le vol de données personnelles », *01.net*, 13/08/19.
[60] ROCHER Luc, HENDRICKS Julien, DE MONTJOYE Pierre-Alexandre, « Estimating the success of re-identifications in incomplete datasets using generative models », *Nature*, 23/07/19.
[61] ROCHER Luc dans « Vos données privées, anonymes ? Jamais totalement, selon des chercheurs UCLouvain », Communiqué de presse UC Louvain, 23/07/2019.

CONCLUSION

Les standards démocratiques et sécuritaires de nos sociétés contemporaines ont été mis à mal. En cause, les données personnelles et leur exploitation frénétique dans un univers numérique peu ou pas sécurisé. Face à l'attrait économique et stratégique qu'elles suscitent, ces données représentent des cibles d'attaques faciles comme l'illustre la multiplication de scandales. De Cambridge Analytica à WannaCry, aucun domaine n'est épargné.

Ainsi, si l'exploitation et la vente de données représentent des opportunités pour les uns, elles symbolisent avant tout des menaces pour les autres. Ces « autres » sont les citoyen-ne-s, premières et souvent principales victimes de ce manque de protection. Dépossédé-e-s voire manipulé-e-s, iels sont exposé-e-s à ces dangers à leur insu. L'enjeu sécuritaire change alors de paradigme, passant de l'individuel au collectif. Ce n'est plus seulement l'individu en tant que tel qui est exposé à des menaces, mais bien la société avec ses normes et ses valeurs démocratiques.

Face à ce constat alarmant, l'UE s'est enfin réveillée avec l'entrée en vigueur du RGPD. La reconnaissance de droits aux utilisateur-rice-s combinée à des obligations sécuritaires dans le traitement des données est une avancée majeure. Néanmoins, les failles sont déjà perceptibles et le décalage entre la lenteur de la norme juridique et la rapidité de l'innovation technologique semble irréconciliable. Dans ce contexte, le système actuel de protection des données semble intrinsèquement précaire face aux multiples enjeux et innovations qui le traversent.

BIBLIOGRAPHIE

DOCUMENTS INSTITUTIONNELS

- Agence Nationale de Sécurité de l'Information, *Rapport d'Activité 2017*, le 26/08/19, Consulté sur : https://bit.ly/2KNlYHg
- Agence Nationale de Sécurité de l'Information, *Rapport annuel 2018*, le 26/08/19, Consulté sur : https://bit.ly/2qHqBpY
- Commission européenne, « Déclaration de M. Ansip, vice-président, et de Mme Jourová, commissaire européenne, à la veille de l'entrée en application du règlement général sur la protection des données », 24/05/2018, Consulté sur : https://bit.ly/2m2hRej
- Commission Européenne, « Règlement général sur la protection des données: bilan de la première année », 22/05/2019, Consulté sur : https://bit.ly/2krYEm8
- Commission Européenne, « Le règlement général sur la protection des données donne des résultats, mais les travaux doivent se poursuivre », 24/07/19, Consulté sur : https://bit.ly/2kpkB5f
- Datatilsynet, Artificial intelligence and privacy. *Report January 2018*, 2018. Consulté sur : https://bit.ly/2K37Q8b
- Institut de l'Internet et du multimédia, *La « data révolution » dans le marketing digital*, 28/10/16. Consulté sur : https://bit.ly/2lHuVpm
- Parlement européen, « Q&R : Les nouvelles règles de l'UE sur la protection des données placent les citoyen-ne-s aux commandes », Background, 01/06/2016. Consulté sur : https://bit.ly/2vodONT
- Parlement européen et Conseil européen, Directive 95/46/CE », Journal officiel des communautés européennes, 24/10/1995, consulté sur : https://bit.ly/2YS7xVD
- Parlement européen et Conseil Européen, *Règlement 2016/679*, Journal officiel de l'Union Européenne, 27/04/2016, Consulté sur : https://bit.ly/2zTZWgk
- The Electoral Commission, « EU referendum results ». Consulté sur : https://bit.ly/2sUrJs8
- Union internationale des télécommunications, « Série Y : Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaines génération. Réseaux de prochaines génération – Cadre général et modèles architecturaux fonctionnels. Présentation générale de l'Internet des objets », *Secteur de la normalisation des télécommunications de l'UIT*, 2012.
- US-CERT, *Alert (TA18-106A) : Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*, 16/04/2018 (mis à jour le 20/04/2018). Consulté sur : https://bit.ly/2H4LXrr

PUBLICATIONS

- ALEXANDRE Laurent, *La guerre des intelligences : intelligence artificielle versus intelligence humaine*, Paris : Jean-Claude Lattès, 2017.
- BAUMARD Philippe, « The behavioral paradigm shift in fighting cybercrime: Counter-measures, innovation and regulation issues », *International Journal on Criminology*, 2(1), 2014, pp.11-22.
- FERRERAS Isabelle, *Firms as Political Entities, Saving Democracy Through Economic Bicameralism*, Cambridge : Cambridge University Press, 2017.
- Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018. Consulté sur : https://bit.ly/2Fdhq4P

- LECUN Yann, BENGIO Yoshua, HINTON Geoffrey, « Deep learning », *Nature*, vol. 521, 28 mai 2015, pp. 436-444
- LUIGGI Jean-Sun, « Cyberguerre, nouveau visage de la guerre ? », Stratégique, vol. 112, n°2, 2016, p.91-100. Consulté sur : https://bit.ly/2qKK1JL
- TROUDE-CHASTENET Patrick, « Fake news et post-vérité. De l'extension de la propagande au Royaume-Uni, aux États-Unis et en France », *Quaderni n°96*, Février 2018
- VINES Paul, ROESNER Franziska, KOHNO Tadayoshi, « Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob », *16e ACM Workshop on Privacy in the Electronic Society*, 30/10/2017. Consulté sur : https://bit.ly/2yBO8ve
- ZAFFAGNI Marc, « Cyberattaque WannaCry : 98% des PC touchés par le ransomware étaient sous Windows 7 », Futura, 22/05/2017. Consulté sur : https://bit.ly/2Hrk6Bd

ARTICLES DE PRESSE ET SITES INTERNET

- ALIX Christophe, « Facebook pris dans la tempête de l'affaire Cambridge Analytica », *Libération*, 20/03/2018. Consulté sur : https://bit.ly/2FbvDiT
- BEZIAT Eric, « 2017, l'annus horribilis d'Uber », Le Temps, le 22/11/2017, Consulté sur : https://bit.ly/2jSeV3d
- BAUSSELER Julien, « Nos objets connectés, mine d'or pour les hackeurs », *Le Soir*, 03/05/2018, p.18
- CADWALLADR Carole, GRAHAM-HARRISSON Emma Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, *The Guardian,* 17/03/2018. Consulté sur : https://bit.ly/2plU1sM
- CHEMINAT Jacques, « Première amende RGPD pour un hôpital portugais », *CIO*, 5/11/2018, Consulté sur : https://bit.ly/2P9PJnf
- CHERIF Anaïs, « Cambridge Analytica : Facebook au cœur d'un nouveau scandale », *La Tribune*, 20/03/2018. Consulté sur : https://bit.ly/2vJuy2l
- Corp, « L'Infographie officielle du Big Data en 10 chiffres clés », 28/02/2019. Consulté sur : https://bit.ly/2lFz25t
- DEARDEN Lizzie, « Russian hackers targeting millions of devices around the world, US and UK warn », *Independent*, 16/04/2018. Consulté sur : https://ind.pn/2qGjjCD
- DELEPINE Justin, « Paris s'attaque à Google et Berlin à Facebook », *Alternatives Économiques*, 1/03/19. Consulté sur : https://bit.ly/2lNCydK
- DECHAMPS Frédéric, DE CLERCQ Chloé, « Tout ce que vous devez savoir sur le RGPD », *Qualifio*, 2018. Consulté sur : https://bit.ly/2HLb9lE
- DELASALLE-STOPER, « Sans Cambridge Analytica, il n'y aurait pas eu de Brexit », *Libération*, 26/03/2018. Consulté sur : https://bit.ly/2E1T11K
- FARINE Mathilde, « La multiplication des données met en péril une vision de la démocratie » , *Le Temps*, 22/05/2017. Consulté sur : https://bit.ly/2Ke4uiM
- FERNANDEZ Manny, ZAVERY Mihir et S. RUEB Emily « Ransomware Attack Hits 22 Texas Towns, Authorities Say », *The New York Times*, 20/08/19. Consulté sur : https://nyti.ms/2KIMoYs
- GALLENBORN Gilbert, « Paradoxalement, le RGPD facilite le vol de données personnelles », *01.net*, 13/08/19. Consulté sur : https://bit.ly/30jddI1
- Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018. Consulté sur : https://bit.ly/2Fdhq4P

- GRAHAM Chris, « NHS cyber attacks: Everything you need to know about the 'biggest ransomware' offensive in history », *The Telegraph*, 20/05/2017. Consulté sur : https://bit.ly/2FGWbKx
- GODARD Bruno, « Comment les publicitaires suivent vos traces sur le Net grâce aux cookies », *Capital*, 29/08/2019. Consulté sur : https://bit.ly/2zA9Ale
- HERRERO Océane, « RGPD: l'Irlande assignée gendarme de l'Union européenne », *l'Opinion*, 19/02/19. Consulté sur : https://bit.ly/2kEDxNp
- L. Bastien, « Uber a caché la fuite de données personnelles de 57 millions d'utilisateurs et de chauffeurs », *Le Big Data*, 23/11/2017. Consulté sur : https://bit.ly/2HxLGN6
- LAZZAROVICI Marianne, « RGPD : quel bilan un an après sa mise en œuvre ? », Toute l'Europe, 8/08/19. Consulté sur : https://bit.ly/2YXcxXo
- LUIGGI Jean-Sun, « Cyberguerre, nouveau visage de la guerre ? », Stratégique, vol. 112, n°2, 2016, p.91-100. Consulté sur : https://bit.ly/2qKK1JL
- *Population Data*, États-Unis, 22/03/2018. Consulté sur : https://bit.ly/2HXnbqv
- Rapid7, National Exposure Index. *Inferring internet security posture by country through port scanning*, 2017; Consulté sur : https://bit.ly/2HQT0n9
- ROCHER Luc, HENDRICKS Julien, DE MONTJOYE Pierre-Alexandre, « Estimating the success of re-identifications in incomplete datasets using generative models », *Nature*, 23/07/19. Consulté sur : https://go.nature.com/2M7oyqE
- ROSE Michael, « What Is Account-Based Marketing? », *Forbes Community Voice*, 01/11/2017. Consulté sur : https://bit.ly/2HGuvcp
- ROSENBERG Matthew, CONFESSORE Nicholas, CADWALLADR Carole, « How Trump Consultants Exploited the Facebook Data of Millions », *The New York Times*, 17/03/2018. Consulté sur : https://nyti.ms/2HH74vA
- RTBF, « Facebook victime d'une nouvelle fuite de données: 540 millions d'utilisateurs concernés », 04/04/2019. Consulté sur : https://bit.ly/2lM8wai
- SCOTT Mark, « Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower », *Politico*, 27/03/2018 (mis à jour le 29/03/2018). Consulté sur : https://politi.co/2Fff9G8
- VINES Paul, ROESNER Franziska, KOHNO Tadayoshi, « Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob », *16e ACM Workshop on Privacy in the Electronic Society*, 30/10/2017. Consulté sur : https://bit.ly/2yBO8ve

Cette publication électronique peut à tout moment être améliorée
par vos remarques et suggestions. N'hésitez pas à nous contacter pour nous en faire part.

POUR LA SOLIDARITÉ - PLS

Fondé par l'économiste belge Denis Stokkink en 2002, POUR LA SOLIDARITÉ - PLS est un European think & do tank indépendant engagé en faveur d'une Europe solidaire et durable.

POUR LA SOLIDARITÉ se mobilise pour défendre et consolider le modèle social européen, subtil équilibre entre développement économique et justice sociale. Son équipe multiculturelle et pluridisciplinaire œuvre dans l'espace public aux côtés des entreprises, des pouvoirs publics et des organisations de la société civile avec comme devise : Comprendre pour Agir.

ACTIVITÉS

POUR LA SOLIDARITÉ – PLS met ses compétences en recherche, conseil, coordination de projets européens et organisation d'événements au service de tous les acteurs socioéconomiques.

Le laboratoire d'idées et d'actions **POUR LA SOLIDARITÉ – PLS**

1. **Mène des travaux de recherche et d'analyse** de haute qualité pour sensibiliser sur les enjeux sociétaux et offrir de nouvelles perspectives de réflexion. Les publications POUR LA SOLIDARITÉ regroupées en sein de trois collections « Cahiers », « Notes d'Analyse », « Études & Dossiers » sont consultables sur www.pourlasolidarite.eu et disponibles en version papier.

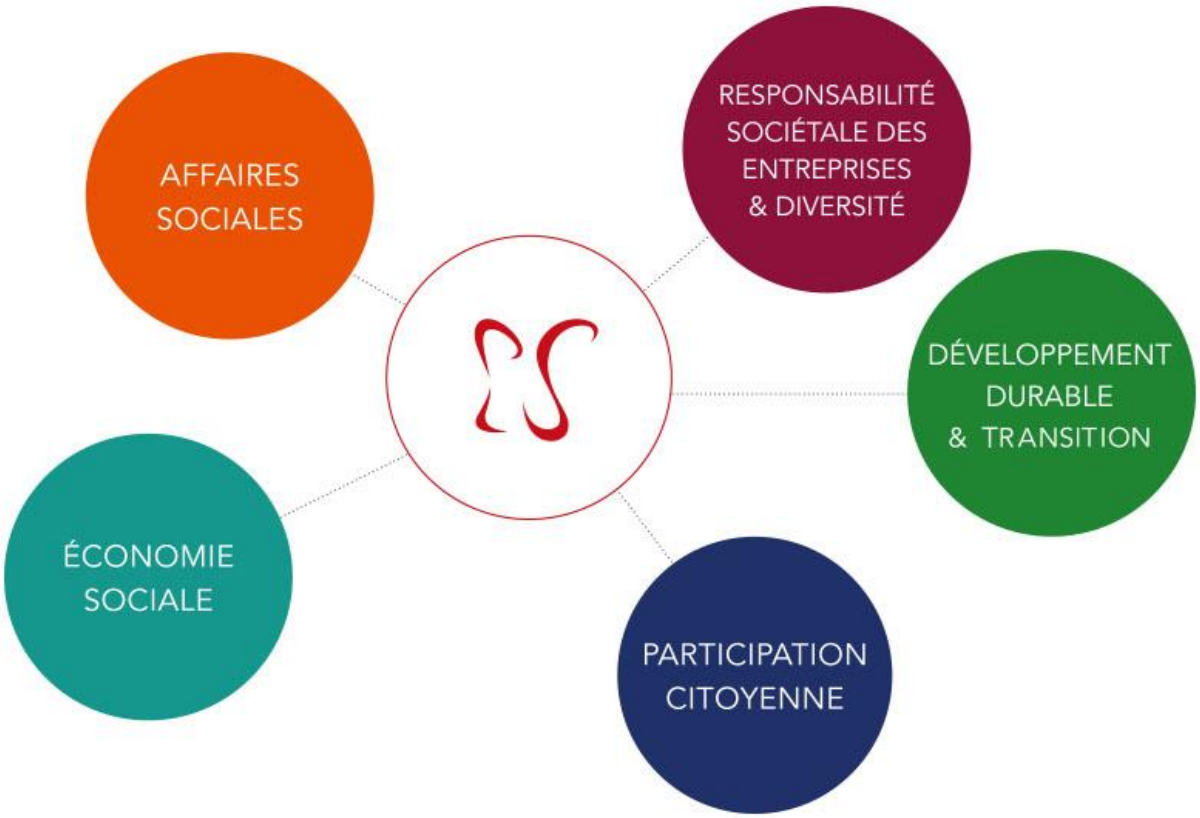
2. **Conseille, forme et accompagne** sur les enjeux européens en matière de lobbying et de financements.

3. **Conçoit et réalise des projets transnationaux** en coopération avec l'ensemble de ses partenaires européens.

4. **Organise des conférences** qui rassemblent dirigeant/e/s, expert/e/s européen/ne/s, acteurs de terrain et offrent un lieu de débat convivial sur l'avenir de l'Europe solidaire et durable.

THÉMATIQUES

POUR LA SOLIDARITÉ – PLS inscrit ses activités au cœur de cinq axes thématiques :



OBSERVATOIRES EUROPÉENS

POUR LA SOLIDARITÉ – PLS réalise une veille européenne thématique et recense de multiples ressources documentaires (textes officiels, bonnes pratiques, acteurs et actualités) consultables via ses quatre observatoires européens:

- www.ess-europe.eu
- www.diversite-europe.eu
- www.transition-europe.eu
- www.participation-citoyenne.eu

COLLECTIONS POUR LA SOLIDARITÉ - PLS

Sous la direction de Denis Stokkink

NOTES D'ANALYSE - *Éclairages sur des enjeux d'actualité*

- *L'inclusion des « Roms » dans l'UE : 2 Notes d'analyse, Safia FALEK, août 2019.*
- *Le développement durable dans l'agenda politique européen, Camille JOSEPH, juillet 2019.*
- *Mobilité durable : 3 Notes d'analyse, Marion PIGNEL, juillet 2019.*
- *La relation Union européenne – Chine : De la naïveté au réalisme, Alexis WILLEMOT, juillet 2019.*
- *Réfugié.e.s LGBTQI+ : les enjeux de la protection internationale, Safia FALEK, juin 2019.*
- *Politique migratoire européenne : de l'asile à l'expulsion ? Anaïs LUNEAU, juin 2019.*
- *La technologie blockchain : une opportunité pour l'économie sociale ? Marion PIGNEL, juin 2019.*
- *Le rôle du Parlement européen dans la conduite des relations extérieures, Safia FALEK, mai 2019.*
- *Du Plan Juncker à InvestEU : les enjeux pour l'économie sociale, Hadrien BARANGER, mai 2019.*
- *L'UE et ses valeurs : mariage de convenance ou divorce en perspective ? Lorelei DEBAISIEUX, mai 2019.*
- *Un programme mondial pour le développement durable, Camille JOSEPH, mai 2019.*
- *Déficit démocratique : un défi pour l'Europe ! Anaïs LUNEAU, avril 2019.*
- *L'Europe sociale : un enjeu de responsabilité collective ! Anaïs LUNEAU, février 2019.*

CAHIERS - *Résultats de recherches comparatives européennes*

- *Vers une économie circulaire en Europe. Anna-Lena REBAUD, septembre 2017.*
- *Face aux nouvelles formes d'emploi, quelles réponses au plan européen ? PLS & SMart, n°36, juin 2017.*
- *Économie sociale, secteur culturel et créatif : vers une nouvelle forme d'entrepreneuriat social en France. PLS & SMart, n°35, mai 2015.*
- *Économie sociale, secteur culturel et créatif : vers une nouvelle forme d'entrepreneuriat social en Wallonie. PLS & SMart, n°34, mai 2015.*
- *Le budget participatif : un outil de citoyenneté active au service des communes. Céline Brandeleer, n°33, octobre 2014.*
- *La Transition : un enjeu économique et social pour la Wallonie. Sanjin Plakalo, n°32, mars 2013.*

ÉTUDES & DOSSIERS - *Analyses et réflexions sur des sujets innovants*

- *Les travailleurs autonomes en Europe : action collective et représentation d'intérêts, Pascale CHARHON, juin 2019.*
- *Enseignement et formation professionnelle en alternance : Vers une filière d'excellence, Marie SCHULLER, décembre 2018.*
- *Politiques de prévention à Bruxelles : Historique et besoins en formation, Marie SCHULLER, septembre 2018.*
- *Les Régions ultrapériphériques : défis et perspectives, Paul HAMMOUD, Antoine MASQUELIN, Tristan THOMAS, février 2018.*
- *Finance et bien-être, une réflexion participative. Marie Leprêtre, décembre 2016.*
- *Pour l'intégration en apprentissage des jeunes vulnérables. Sanjin Plakalo, décembre 2016.*
- *La participation des travailleurs au sein des entreprises. Denis Stokkink, novembre 2016.*

Toutes les publications POUR LA SOLIDARITÉ - PLS sur www.pourlasolidarite.eu

Participation citoyenne

POUR LA SOLIDARITÉ – PLS mène des initiatives plurielles pour renforcer la démocratie participative, la participation citoyenne à la vie politique, l'intégration des personnes immigrées ou d'origine immigrée, la lutte contre les discriminations. En guise de fil conducteur, POUR LA SOLIDARITÉ-PLS opte pour des activités qui, de manière directe ou indirecte, motivent les habitant-e-s de tout État européen à devenir acteur et actrice de cette citoyenneté européenne afin d'instaurer un plus large dialogue entre les pouvoirs publics, la société civile et les entreprises et ainsi bâtir à l'horizon 2020 une Union européenne inclusive.

Collection « Notes d'analyse » dirigée par Denis Stokkink

www.pourlasolidarite.eu

Avec le soutien de

Wallonie

FÉDÉRATION WALLONIE-BRUXELLES

RÉGION DE BRUXELLES-CAPITALE

Francophones Bruxelles