Fondation Jean Jaurès

Société

LE RGPD, DIX-HUIT MOIS APRÈS : QUEL BILAN ?

Thomas Chevandier

25/10/2019

Voilà près de dix-huit mois que le Règlement général sur la protection des données (RGPD) est entré en vigueur. Pour Thomas Chevandier, le regard rétrospectif que l'on porte sur cette période nous permet de conclure à son efficacité relative en matière de protection des données : les sociétés exploitant les données contournent facilement les règles et les autorités de régulation sont trop faibles pour protéger les libertés individuelles. Il apparaît en outre que le RGPD ne constitue pas la réponse appropriée pour lutter efficacement contre l'influence grandissante des GAFA et des sociétés asseyant leur pouvoir immense sur le contrôle et l'usage des données.

En 2014, le Conseil d'État consacrait son étude annuelle aux relations entre le numérique et les droits fondamentaux. Il s'attachait alors à déblayer la question de la pénétration du droit, en tant qu'ensemble normatif et contraignant, dans des espaces numériques dont la culture dominante est à la fois libertaire et libérale. Libertaire dans le sens où Internet a été vu par de nombreux militants comme un espace libéré de toute institution normative ou dépositaire d'une contrainte légitime. Cette culture est aussi libérale parce que cette absence de règles contraignantes a permis l'émergence de nouveaux marchés, en dehors de toute régulation économique. De ces nouveaux marchés, quelques sociétés ont émergé et constituent aujourd'hui des géants dont on se demande comment les mettre au pas.

La haute juridiction administrative présentait ainsi l'enjeu :

> « La saisie croissante du numérique par le droit est à la fois une réalité et une nécessité. Elle doit être portée à un niveau supranational, d'abord à l'échelle européenne par la définition d'un socle commun de règles impératives, ensuite au niveau transatlantique en vue d'une gouvernance plus équilibrée et plus efficace des flux numériques. [...] Des choix stratégiques devront être opérés et une sécurisation juridique des usages du numérique, notamment en matière de données personnelles, est encore à assurer. »

Le Conseil d'État plaçait donc au cœur de la question de la régulation d'Internet celle de la protection des données personnelles. La circulation de ces dernières soulève, en effet, une double problématique : d'une part, la mise à disposition des données personnelles s'appréhende au regard de la protection des libertés fondamentales et, plus spécifiquement, de la vie privée ; d'autre part, les données constituent la matière première à la source du pouvoir et de la richesse des GAFA.

Partant, la définition d'un régime juridique de contrôle, de régulation et de protection des données personnelles est théoriquement censée répondre à un double enjeu : en premier lieu, protéger la vie privée des milliards d'usagers d'Internet ; en second lieu, limiter la puissance sans cesse croissante de sociétés privées qui viennent bousculer tous les marchés économiques, concurrencer les États et mettre en danger les démocraties.

Ainsi défini par ce caractère bicéphale, le problème de la protection des données personnelles nous renvoie à des débats et des clivages dont nous sommes finalement familiers : d'un côté, la protection des libertés individuelles par la définition d'un socle de droits au bénéfice des individus ; de l'autre, la protection de l'intérêt général par l'encadrement du marché des données.

Le RGPD s'inscrit pleinement dans la première logique en ce qu'il détermine et organise la protection d'un socle de droits visant à protéger, principalement, la vie privée des usagers européens d'Internet. La première partie de la présente étude visera donc à déterminer, grâce au recul de dix-huit mois de mise en œuvre, si le RGPD constitue un régime juridique permettant de protéger efficacement les droits des personnes.

Il sera ensuite, en seconde partie, fait état des angles morts du RGPD et des enjeux auxquels il ne répond pas, notamment dans l'objectif de lutter contre le pouvoir des GAFA. Ces réflexions ont pleinement leur place dans un premier bilan du RGPD, ce dernier ne pouvant finalement être considéré autrement que comme une première étape de la soumission du monde du numérique au droit, c'est-à-dire à l'intérêt général.

Le RGPD : bref rappel des principales nouveautés

Avant d'interroger le bilan de cette nouvelle réglementation, rappelons ce qu'elle a changé, notamment en France, qui faisait figure de pionnière en matière de protection des données depuis la loi de 1978 et la création de la CNIL (Commission nationale de l'informatique et des libertés).

Une définition large des données personnelles. Le RGPD ne concerne que les données personnelles, définies comme « toutes les informations identifiant directement ou indirectement une personne physique ». Cette définition permet de rattacher à la notion un ensemble de données très diversifié, qu'il s'agisse d'un nom, d'un numéro d'immatriculation (votre numéro de carte Vitale est une donnée personnelle), une photographie, une empreinte digitale, etc. C'est donc l'acception large de la notion qui a été retenue, donnant à la nouvelle réglementation un champ d'application très (trop ?) large.

Une responsabilisation accrue des organismes exploitant des données. Le RGPD vise à renverser la logique de mise en conformité des organismes au RGPD. Avant, chaque partie qui tenait un fichier avec des données personnelles devait le déclarer à la CNIL, qui autorisait sa mise en œuvre. Désormais, l'organisme doit se mettre en conformité avec la nouvelle réglementation par lui-même, sans formalité ou déclaration préalables de ses traitements par l'autorité de contrôle. En conséquence, toute personne exploitant des données personnelles doit désormais mettre en œuvre des procédures internes pour limiter l'usage des fichiers et, en tout cas, veiller à ce qu'elles respectent le nouveau cadre juridique. Elle doit également nommer un délégué à la protection des données, revoir tous ses contrats avec les partenaires, reprendre et mettre à jour les procédures de sécurisation des systèmes informatiques, etc.

Un renforcement des droits des personnes. C'est là la véritable promesse du RGPD et sa partie la plus visible, celle qui concerne et affecte tous les utilisateurs.

• Une meilleure protection du consentement et un renforcement de la transparence. Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible. En ce sens, les utilisateurs doivent être informés de l'usage qui est fait de leurs données, ils doivent pouvoir donner leur accord pour le traitement ou pouvoir s'y opposer.

• Un droit à la portabilité des données et un droit à l'oubli. Ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers.

• La possibilité d'introduire des actions collectives. Le RGPD autorise les actions de groupe visant à obtenir la cessation d'un manquement, dans le cadre d'actions menées par des organisations mandatées.

• Un droit à la réparation du préjudice moral ou matériel. Toute personne ayant subi un dommage du fait d'une violation du règlement a le droit d'obtenir du responsable de traitement ou du sous-traitant réparation du préjudice.

Un renforcement des sanctions. Le montant des sanctions qui peuvent être prononcées par les autorités nationales de régulation a été relevé à 20 millions d'euros ou, pour les sociétés, à 4% de son chiffre d'affaires annuel mondial.

Premier bilan du RGPD : entre prise de conscience mondiale et mise en œuvre kafkaïenne

Le RGPD est partout, il a envahi notre vie. Sans même parler de l'intense couverture presse du mois de mai 2018, on pense surtout, dans notre vie privée, à son impact à chaque connexion sur un site Internet où il nous est demandé de consentir au dépôt de cookies et à l'ensemble des mails reçus par les éditeurs des newsletters, par lesquels on se voit préciser la politique de mise en conformité. Quant à notre vie professionnelle, ou militante, ou engagée, combien de mises en garde de nos hiérarchies, de nos clients, de nos prestataires, de nos services informatiques ?

Alors, au-delà de ces interpellations, qu'en est-il véritablement ? Le nouveau régime juridique

protège-t-il effectivement nos droits ? Les responsables des millions de traitements de données personnelles se sentent-ils véritablement contraints au point de perdre en rentabilité ou en efficacité pour se mettre en conformité avec le RGPD ?

Cette première partie vise à répondre à cette question en étudiant l'efficacité du RGPD au regard des moyens dont dispose la puissance publique pour faire respecter les nouveaux droits.

Le RGPD, une révolution culturelle ?

Les premières indications sur l'impact du RGPD sur l'opinion publique nous sont données par un sondage Ifop, commandé et publié par la CNIL. Effectué fin octobre 2018, soit près de six mois après l'entrée en vigueur du RGPD, il nous donne des indications plus approfondies sur le ressenti des Français vis-à-vis du règlement général.

On y apprend notamment que 66% des personnes interrogées se déclarent aujourd'hui « plus sensibles à la question de la protection des données personnelles » qu'auparavant et que 59% considèrent que les données personnelles sont insuffisamment protégées. Pour autant, le RGPD est perçu très largement (73%) comme étant un outil efficace pour « protéger les données personnelles des citoyens et des consommateurs », alors que seuls 39% y voient une « contrainte supplémentaire pour les entreprises, qui n'est pas nécessaire ». Ainsi, les sondés font primer très largement la protection de leurs droits à l'intérêt économique, ce qui distingue ce sujet de nombreux autres où l'efficacité économique prime de plus en plus sur la volonté de défense de droits ou de préservations d'acquis, notamment dans les domaines sociaux ou en droit du travail.

Ce premier aperçu de l'état de l'opinion à l'endroit de la protection des données personnelles est largement confirmé par l'ensemble des informations fournies par la CNIL dans son bilan d'activité 2018, présenté le 15 avril dernier. L'autorité de régulation précise ainsi qu'il y a eu 8 098 232 visiteurs sur le site de la CNIL en 2018, soit une augmentation de 80% par rapport à 2017. Certaines pages du site ont été consultées plusieurs centaines de milliers de fois, comme « RGPD : se préparer en six étapes » (888 604 vues), ou encore l'article « RGPD : ce qui change pour les professionnels » (377 630 vues). On peut continuer longtemps la liste des pages consultées plus de 100 000 fois sur le site de la CNIL.

Cet intérêt se confirme lorsque l'on s'intéresse aux statistiques des personnes entrées en contact avec la CNIL : elle a ainsi reçu, pour l'année 2018, 189 877 appels, essentiellement en provenance de particuliers souhaitant exercer leurs droits ou obtenir des conseils sur la meilleure manière d'y parvenir. Ces chiffres témoignent d'un intérêt qui dépasse la simple communauté des « geeks »

(qui sont d'ailleurs rarement les premiers à se renseigner sur les sites institutionnels) ou des délégués à la protection des données. Plus encore, ils semblent attester du fait que l'attention portée au RGPD va plus loin qu'une curiosité du moment et s'apparente à une prise de conscience de l'existence de nouveaux droits et d'une volonté de les préserver.

Une faible hausse du nombre de plaintes déposées à la CNIL

Le nombre de plaintes déposées à la CNIL constitue un premier indicateur permettant de déterminer dans quelle mesure cette prise de conscience peut avoir des conséquences opérationnelles pour les acteurs et les responsables de traitements et, ainsi, accélérer le changement. Il est, en effet, possible d'adresser des réclamations à la CNIL dans deux cas. En premier lieu, quand on ne parvient pas à exercer ses droits, par exemple lorsque l'on demande une copie de ses données à un responsable de traitement (votre banque, un réseau social, votre mairie, etc.) et que la demande reste sans réponse depuis plus d'un mois. En second lieu, dans les cas où l'on soupçonne ou constate une atteinte aux règles de protection des données. On pense alors au cas typique de la newsletter d'un organisme que l'on reçoit alors qu'on ne lui a jamais communiqué ses données. On peut également citer le cas des employés qui constatent l'installation d'un système de vidéosurveillance sans en avoir été avertis par leur employeur.

La procédure est alors relativement simple puisque la CNIL a élaboré un téléservice de plainte en ligne plutôt intuitif, sur lequel on peut télécharger facilement les pièces à l'appui de sa réclamation. Sur l'ensemble de l'année 2018, 11 077 plaintes ont été enregistrées sur le site de la CNIL, contre 8 360 l'année précédente. Sur l'ensemble de ces plaintes, 9 310 ont fait l'objet d'une instruction approfondie par les services de la CNIL, qui peut se traduire par de simples questions posées au responsable du traitement, à des visites et des contrôles sur site.

En conséquence, si l'on note une hausse du nombre de plaintes, d'autant plus significative que seule la moitié de l'année 2018 est concernée par la mise en œuvre du nouveau régime juridique, on n'en constate pas pour autant une explosion. À titre de comparaison, la hausse semble même s'inscrire dans une trajectoire plus globale d'augmentation constante des plaintes à la CNIL : 5 802 en 2014, 7 908 en 2015, 8 360 en 2017.

Si l'on traite des effets juridictionnels dans les paragraphes qui suivent, on ne peut, à ce stade, que constater un grand moment de prise de conscience européenne des droits des personnes en matière de protection des données qui a accouché d'une hausse relative de 24% des réclamations en ligne. On peut certes y voir l'amorce d'un mouvement irréversible dont les premiers effets tardent à être visibles du fait du décalage entre prise de conscience et actes objectifs. À l'inverse,

on peut considérer que c'est bien peu, compte tenu de la bulle médiatique entretenue dans tout le second semestre de l'année 2018, et que même le feu de paille avait une vigueur relative.

Les moyens limités de la CNIL, obstacle structurel à la protection effective des droits des personnes

Avec à peine 200 agents (seulement 22 de plus qu'en 2013, ce qui ne témoigne pas d'un effort budgétaire significatif de la part de l'État – le budget global de la CNIL ayant même diminué depuis 2016 –, et avec seulement une petite partie des agents affectés aux contrôles, la CNIL n'a pas les moyens d'effectuer de nombreux contrôles, ni même de particulièrement les approfondir.

Ainsi, sur l'année 2018, la CNIL a effectué 310 contrôles, dont 204 sur place, 51 en ligne et 51 sur pièces. La liste de ces contrôles est d'ailleurs publiée sur le site Data.gouv.fr et fait état d'une volonté de la CNIL d'atteindre tous les types de structures et de secteurs d'activité : par exemple, on a de petits commerçants (une petite auto-école parisienne, un hôtel à Villemonble), un lycée de Vitry-sur-Seine, une entreprise de pompes funèbres à Lambersart, des communes, des services régaliens, etc.

La CNIL identifie trois types d'éléments déclencheurs à ces contrôles. D'abord, ce sont les failles de sécurité qui sont à l'origine d'un grand nombre de contrôles. Ensuite, les questions de vidéoprotection sont au cœur des investigations de la CNIL, qui a, par exemple, effectué des contrôles de radars sur lesquels elle vérifiait la durée de conservation des plaques d'immatriculation. Dans le même sens, elle a contrôlé les dispositifs de caméras individuelles que portent les policiers lors de leurs interventions. Enfin, la troisième source de contrôles est l'utilisation abusive de données par des services commerciaux de prospection.

Sur l'ensemble de ces contrôles, 57% sont initiés par la CNIL elle-même, au regard de l'actualité, et seulement 22% sont la conséquence d'une plainte ou d'un signalement. Cette dernière statistique mérite d'être soulignée : sur l'ensemble des plaintes mentionnées ci-dessus, seules 68 d'entre elles ont abouti à un contrôle. Le RGPD étant présenté comme l'outil de réappropriation de leurs données par les citoyens avec le soutien de la puissance publique et, plus singulièrement, des autorités de contrôle, ce maigre bilan relativise sensiblement la portée du fameux règlement.

Il est vrai que la CNIL dispose de moyens relativement limités et l'on comprend que sa politique de sanctions, par laquelle elle vise désormais quelques contrevenants symboliques auxquels elle inflige de lourdes sanctions, a une visée préventive. Mais on ne peut manquer de souligner la faiblesse de cette statistique : le grand chambardement du droit des données, annoncé dans la

presse durant des mois, pour lequel les usagers du net ont été sensibilisés comme jamais, débouche sur 68 maigres contrôles.

Une politique de sanctions inefficace avant l'entrée en vigueur du RGPD

Il a été rappelé ci-dessus l'intérêt stratégique de l'effet dissuasif de la sanction : face à l'océan des fichiers, une CNIL avec des moyens limités et qui ne progressent pas est dans l'obligation de mener une politique de sanctions d'envergure, ciblées et symboliques, pour que les responsables de traitements se sentent contraints de faire appliquer les grands principes du RGPD.

Les sanctions pécuniaires doivent être suffisamment importantes pour que les acteurs économiques dont les données personnelles sont la principale matière première aient un intérêt économique à changer leurs comportements. Pour être concret, on comprendra qu'une société tirant 10 millions d'euros d'une utilisation abusive d'un fichier continuera de l'exploiter si elle ne risque qu'une amende de 1 million d'euros.

Il est d'abord surprenant de constater que les mises en demeure (qui ne sont d'ailleurs pas des sanctions à proprement parler) sont en nette diminution en 2018 : 93 en 2015, 79 en 2017 et 48 en 2018 ! On peut expliquer ce chiffre de deux manières : d'une part, depuis la loi du 20 juin 2018, la mise en demeure n'est plus un préalable nécessaire à la sanction ; d'autre part, si elles sont en diminution, le nombre de mises en demeure publiées a, lui sensiblement augmenté, passant de 3 en 2017 à 13 en 2018, transformant ainsi la mise en demeure en sanction douce. En effet, une société dont la mise en demeure par la CNIL est publiée subit un préjudice d'image non négligeable, notamment s'agissant de sociétés dont le modèle économique est structuré autour de l'usage de données.

On est donc passé par les filtres multiples de la plainte, du contrôle et de la mise en demeure, sur le long chemin qui nous mène au prononcé d'une sanction par la CNIL. Et, arrivé là, on constate qu'il reste finalement peu de monde**.** Avec des centaines de milliers de fichiers constitués en France, plus de 11 000 signalements effectués à la CNIL, on arrive au prononcé de seulement 10 sanctions pécuniaires en 2018. Sur ces 10 sanctions, 7 concernent des atteintes à la sécurité des données. Quant au montant des sanctions, il a sensiblement augmenté pour atteindre un total de 1 196 000 euros en 2018, contre 371 000 en 2017, sachant que les nouveaux plafonds de sanctions de la CNIL n'étaient pas encore appliqués. Ainsi, l'amende maximale en 2018 concernait Uber et avait été fixée à 400 000 euros, en raison d'une faille de sécurité ayant affecté 1,4 million d'utilisateurs en France.

À ce stade, on peut considérer que l'effet préventif des sanctions de la CNIL n'apparaît pas

clairement. Sur des centaines de milliers de traitements de données, plus de 11 000 plaintes, seulement 9 sanctions, dont la plus élevée est de 400 000 euros : la faiblesse quantitative et qualitative de ces sanctions laisse relativement sceptique quant à l'effectivité du droit de la protection des données personnelles.

Cependant, ces sanctions ont été prononcées quand la loi antérieure était en vigueur, depuis le RGPD a largement rehaussé les plafonds d'amendes, celles-ci pouvant désormais atteindre un montant de 20 millions d'euros ou, dans le cas d'une entreprise, 4% de son chiffre d'affaires mondial. Une première sanction pécuniaire a d'ailleurs été prononcée sous l'empire des nouvelles dispositions, début 2019, donnant une indication de la nouvelle doctrine de la CNIL en la matière.

La sanction prononcée contre Google : un tournant ?

La décision du 21 janvier 2019, par laquelle la CNIL a prononcé une sanction de 50 millions d'euros à l'encontre de Google est doublement historique, d'une part, par la procédure qui a été utilisée pour y parvenir : pour la première fois, la CNIL a prononcé une sanction au moyen de la procédure de la plainte collective (voir encadré). Ainsi, près de 10 000 personnes avaient mandaté La Quadrature du Net pour saisir la CNIL d'une plainte contre Google, sur le fondement du défaut de base juridique pour le traitement des données des utilisateurs à des fins de personnalisation de la publicité. D'autre part, elle est historique par le montant de la sanction, qui est plus de 100 fois supérieur à la précédente sanction record (400 000 euros à Uber). Cette sanction constitue en vérité un véritable tournant dans la politique de sanctions de la CNIL, qui va compenser la faiblesse de ses moyens par la peur qu'elle pourra susciter pour les responsables de traitements. Il est donc beaucoup trop tôt pour avoir du recul sur les effets de cette sanction, mais elle témoigne d'une volonté de la CNIL de frapper fort, et sur des cibles symboliques.

En ce sens, personne ne doit se sentir à l'abri, et les cibles symboliques ne manquent pas : elle pourrait sanctionner lourdement un parti politique qui serait coupable de manquements caractérisés ; elle pourrait s'en prendre à une collectivité ou à une entreprise publique, etc.

La présidente de la CNIL a d'ailleurs tenu à donner un sens à cette sanction et à celles qui suivront : « Nous avons toujours une volonté d'accompagnement forte mais, à partir de maintenant, c'est la fin d'une certaine forme de tolérance, un an après l'entrée en vigueur du RGPD. L'accompagnement ne serait pas crédible sans contrôle assorti, le cas échéant, de sanctions. »

Pour autant, l'impact de cette doctrine en construction de la CNIL et, par conséquent, de la mise en

œuvre effective du RGPD par les acteurs économiques et l'ensemble des responsables de traitements en France dépendra très largement de la position du Conseil d'État, juridiction d'appel des décisions de la CNIL.

Google ayant fait appel, il est tout à fait envisageable que le Conseil d'État décide de réformer ladite décision, notamment pour des raisons de compétence territoriale de la CNIL. C'est surtout s'il se prononce sur le fond que l'arrêt du Conseil d'État sera regardé avec intérêt, notamment sur le montant de la sanction. Rappelons qu'il n'a pas hésité, encore très récemment, à réformer une décision de la CNIL en diminuant légèrement le montant de l'amende (de 250 000 euros à 200 000 euros), au motif que la CNIL n'avait pas tenu compte des efforts effectués par la société sanctionnée pour se mettre en conformité.

Neuf mois après son prononcé, il apparaît que la sanction contre Google constitue plus un tournant qu'un acte isolé. La CNIL britannique a prononcé, en juillet dernier, une sanction administrative de 110 millions d'euros contre le groupe Marriott, auquel il est reproché un certain nombre de négligences dans la sécurisation de ses infrastructures informatiques ayant conduit à la fuite de données sur 339 millions de clients, dont 7 millions de Britanniques. British Airways a également été condamnée au versement d'une amende de 204 millions d'euros, soit 1,5% de son chiffre d'affaires, à la suite de la découverte d'une faille de sécurité.

La surexposition du RGPD et son identification comme outil de régulation de l'usage des données personnelles sont, un an et demi après son entrée en vigueur, indéniables. Dans le même sens, on perçoit un mouvement de mise en conformité de nombreux organismes, à travers, notamment, le nombre croissant de nominations des délégués à la protection des données.

Pour autant, après un an et demi de mise en œuvre, les premières limites du RGPD sont parfaitement perceptibles. En ce sens, rien n'indique que la CNIL sera en mesure d'accroître ses contrôles pour vérifier de façon effective que les responsables de traitements respectent bien les règles. Quant aux sanctions, il est à craindre que leur grande rareté, rendue structurelle par le manque de moyens de la CNIL, atténue le caractère incitatif de la hausse des plafonds de sanctions, dont l'amende prononcée contre Google constitue le premier exemple. Sans compter que l'on ne sait pas encore quelle sera l'attitude du Conseil d'État et s'il suivra le CNIL sur le montant des sanctions.

C'est d'ailleurs ces considérations qui ont conduit, récemment, La Quadrature du Net à attaquer la CNIL devant le Conseil d'État. Il est ainsi reproché à l'autorité de régulation d'être trop flexible, notamment s'agissant des cookies, pour lesquels elle a mis en place un régime transitoire devant

aller jusqu'en 2020, en violation du RGPD.

Il est ainsi à craindre que le grand mouvement de mise en conformité concerne en premier lieu les « petits », à savoir les petites associations, les collectivités publiques, les PME. Ainsi, tous ceux qui ne font pas commerce de nos données joueraient le jeu, là où le RGPD semblerait insuffisant pour cadrer les pratiques des nouveaux géants du numérique, de ceux qui font commerce de nos données, mettent en danger nos vies privées ou cherchent à agir sur nos comportements.

Car, à l'image des coureurs cyclistes qui ont longtemps eu un temps d'avance sur les organismes chargés de la lutte contre le dopage, ces derniers font preuve d'imagination pour contourner les nouvelles règles tout en échappant à la sanction.

L'utilité limitée du RGPD dans le combat de la puissance publique contre les GAFA

Cette première partie de l'étude, qui porte sur la mise en œuvre juridique et pratique du RGPD doit être mise en relation avec le rôle social, économique et politique pris par les données.

Plus précisément, il s'agit de savoir si ce régime juridique, dont on vient de souligner les imperfections et l'ambivalence des premiers résultats, constitue un encadrement, une régulation suffisante pour limiter la puissance des GAFA, pour redonner du champ à la puissance publique et pour permettre aux individus de retrouver le contrôle de leurs données personnelles.

« Le capitalisme de la surveillance » et le pouvoir sans limite des GAFA

Shoshana Zuboff, professeur à Harvard, vient de publier un ouvrage, *The age of surveillance capitalism*, dont le succès met en lumière des thèses que l'on pourrait qualifier de critique marxiste de la société numérique et de la nouvelle accumulation capitalistique qu'elle induit. La revue *Esprit* vient notamment d'en publier un extrait traduit qui permet de mieux l'appréhender.

Elle désigne par « capitalisme de surveillance » l'économie de la captation et du traitement des données par les géants du numérique, découverte par Google en 2001 lorsque la société a décidé d'utiliser les données fournies par les utilisateurs de son moteur de recherche pour proposer des prestations de ciblage publicitaire ultra-personnalisé.

L'immense succès financier que constitue ce choix a inspiré les futurs géants qui ont pensé et développé, au tournant des années 2010, des outils leur permettant de récupérer un maximum de

données dans le but d'alimenter leurs systèmes de publicités ciblées. C'est ainsi qu'est né le fameux bouton « Like » de Facebook, dont l'objet est de récupérer le maximum de données personnelles des utilisateurs. Chaque profil ou article liké apportent un capital supplémentaire pour Facebook et offrent la possibilité d'un ciblage publicitaire plus précis et donc plus cher aux annonceurs.

Les « assistants personnels », désormais commercialisés à grande échelle, ne sont ainsi pas un don des grandes firmes qui nous permettent d'éteindre la lumière sans bouger du canapé, ou de contrôler son thermostat à distance. C'est un moyen pour les Google, Amazon et Apple, qui en sont les principaux producteurs, d'aller chercher des données plus personnelles, plus secrètes et plus intimes. D'autres produits plus ciblés permettent de découvrir l'immense imagination dont font preuve les concepteurs des produits, dont le but caché, derrière l'apparence du service rendu à l'utilisateur, consiste à amasser de la donnée sur son sujet. Shoshana Zuboff prend l'exemple de la bouteille de vodka intelligente qui permet de connaître votre consommation d'alcool, ou encore du thermomètre rectal connecté qui diffuse des données de santé.

Toutes ces données, dont l'accumulation par les grands groupes est exponentielle, nourrissent des algorithmes permettant de prédire les comportements, voire de les orienter.

Le regroupement de ces données constitue un capital cumulé par les entreprises en question qui, d'une part, produit des richesses immédiates par les revenus publicitaires engendrés, et, d'autre part, leur offre un avantage compétitif permettant d'élargir sans cesse leurs revenus, leur capacité d'investissement et de rachat des futurs concurrents.

Les thèses de Shoshana Zuboff éclairent le rôle joué par les données personnelles dans la construction des GAFA et introduisent une première critique marxisante de la dynamique de ces dernières.

On comprend donc que la question de la régulation de la circulation des données personnelles constitue un danger gigantesque pour ces firmes, dont l'essentiel du capital est constitué de données personnelles qu'ils ont réussi à monétiser.

Le RGPD devra donc être jugé sur le long terme sur sa capacité à devenir un outil juridique de régulation et d'encadrement de ces géants, à la fois pour protéger nos vies privées, mais également pour limiter leurs pouvoirs.

Les manifestations de l'insuffisance du RGPD à contrer le pouvoir les GAFA

L'empressement de Facebook à défendre le RGPD rend ce dernier suspect quant à sa capacité à constituer une première base de la riposte des autorités publiques à la puissance croissante des GAFA.

De fait, et s'il vient d'être précisé ci-dessus que l'efficacité des principes du RGPD dépendra en grande partie de l'ampleur des sanctions prononcées par les autorités de régulation à l'endroit des contrevenants, un exemple témoigne d'un grand décalage entre la prise de conscience généralisée relative à l'importance de protéger ses données et l'absence de changement de comportement des utilisateurs.

Chacun a pu constater que, depuis l'entrée en vigueur du RGPD, l'utilisateur doit consentir au dépôt de cookies par le site en question sur son ordinateur ou sur son smartphone. Ces cookies sont des aspirateurs à données, des sortes de microespions qui viennent s'installer sur votre terminal et transférer des informations à votre sujet à l'éditeur du site Internet. Il y a plusieurs sortes de cookies, certains servent seulement à mesurer l'audience d'un site et en faciliter la navigation. Mais, dans d'autres cas, ils permettent de capter des données personnelles qui seront ensuite monnayées, selon le schéma décrit par Shoshana Zuboff.

Les cookies déposés sur vos ordinateurs sont donc un élément structurant du « capitalisme de surveillance » qu'analyse cette dernière. Dès lors, on pourrait considérer que le RGPD constitue une avancée formidable en ce qu'il interdit, notamment, le dépôt de cookies (en dehors de quelques exceptions, liées à la base légale du traitement de données), à moins que l'utilisateur ne donne son consentement. Le cas des cookies serait ainsi l'exemple d'une prise de contrôle de leurs propres données par les personnes concernées.

Cette possibilité de reprise de contrôle, conjuguée à la prise de conscience généralisée sur les enjeux liés aux données personnelles, devrait, en toute logique, aboutir à ce que les utilisateurs prennent le temps de vérifier quels cookies ils acceptent et d'en refuser certains ou, *a minima*, de les reconfigurer. Or, selon une étude menée par Tead's, un cabinet de conseil spécialisé dans le numérique, 95% des internautes donnent automatiquement leur consentement au dépôt de traceurs sur leur terminal. Ce chiffre témoigne en lui-même d'une chose : l'utilité relative du principe du consentement préalable au traitement des données pour encadrer l'expropriation des données personnelles et sa captation continue et à grande échelle par les géants du numérique.

On pourrait aller plus loin et souligner, comme le font Maxime des Gayets et Chloé Morin dans une étude publiée par la Fondation Jean-Jaurès, l'usage de biais cognitifs par les géants du numérique

pour contourner les prescriptions du RGPD. Ils font référence, notamment, à une étude publiée en 2018 par l'agence norvégienne de défense des consommateurs, selon laquelle Facebook, Google et Windows 10, notamment, utilisent « des stratagèmes pour nous décourager d'exercer nos droits à la vie privée ». Ainsi, le chiffre des 95% d'acceptation du dépôt de traceurs devrait être interprété non pas comme le résultat d'une sorte de servitude volontaire, mais plutôt le produit d'une manipulation parfaitement consciente de ceux qui font commerce de nos données.

En somme, cette statistique sur le taux d'acceptation de cookies suffit à elle seule à poser la limite intrinsèque du RGPD dont la clé de voûte est, justement, la protection du consentement préalable. Or, avec des utilisateurs qui renoncent presque systématiquement à cet outil de protection, c'est la clé de voûte qui fait défaut, et tout l'édifice qui s'effondre.

Le pouvoir des données, un danger immédiat pour la démocratie auquel le RGPD ne permet pas de répondre

Si l'on vient d'étudier la question de l'origine des données comme matière première, ou plutôt comme capital immatériel central dans le développement et dans la prise de pouvoir des grands groupes, il convient maintenant d'aller à l'autre bout de la chaîne et de voir les risques que le traitement des données fait peser sur la démocratie.

Le scandale Cambridge Analytica a montré que le traitement de données personnelles de masse par l'intelligence artificielle permettait d'influencer une élection, notamment au moyen d'une technique appelée « microciblage ».

L'analyse la plus intéressante de la technique a été publiée par un groupe interdisciplinaire de chercheurs hollandais, dans la *Utrecht Law Review*, dans un article intitulé « Online Political Microtargeting : Promises and Threats for Democracy ». Le microciblage y est décrit comme la surveillance du comportement des internautes et l'utilisation des données collectées afin de leur faire parvenir, à intervalle régulier, des publicités politiques ciblées.

Les risques sont, dès lors, multiples pour le bon fonctionnement de la vie démocratique. D'une part, l'usage non contrôlé de données personnelles *via* les techniques de microciblage constitue une technique de manipulation de l'opinion et de l'électorat. Pratiquée à grande échelle, liée à la diffusion de *fake news*, elle permet à ces dernières de mieux prospérer et d'infuser. Pratiquée sur des publics plus déterminés, notamment l'électorat identifié comme volatile des petits *Swing States*, les personnes ciblées sont harcelées de messages au point de forcer son vote et de faire basculer une élection qui se joue à la marge.

Si le microciblage permet d'orienter le vote, il compromet aussi le secret du vote *via*le traitement de données de masse permettant de déduire le comportement électoral des personnes. Les auteurs soulignent un autre risque lié à l'usage de ces techniques. Le principe même de la démocratie et de la politique est son caractère public et repose dans la nécessité de convaincre une majorité autour d'un projet utile à l'intérêt général, or, le microciblage est, au contraire, un moyen de communication politique opaque puisqu'il vise à diffuser un message uniquement à certaines catégories de personnes, sur des espaces publicitaires qui ne sont vus que d'eux-mêmes. On est loin du spot TV, censé embrasser la nation entière, diffusé à une heure de grande écoute. De même, ces techniques, qui permettent de cibler le message politique en fonction des catégories de personnes auxquelles le candidat ou le parti souhaite s'adresser, tendent à essentialiser la vie politique. Il n'est plus question de chercher à construire un discours qui rassemble et à bâtir un projet qui fédère puisque le ciblage permet de flatter ce qui distingue et que c'est électoralement plus efficace.

Dans son ouvrage critique consacré aux GAFA, Scott Galloway analyse un pan ignoré de leur pouvoir, considérant qu'ils sont maintenant des plates-formes de circulation de l'information et de sélection de contenus. Ils sont devenus, notamment Facebook et Google, les principales plates-formes de médias, éclipsant, en audience, les grands médias traditionnels.

Paul Nemitz, haut fonctionnaire à la Commission européenne et professeur au Collège d'Europe de Bruges, analyse cette nouvelle forme d'influence à l'aune des moyens traditionnels et constitutionnels du contrôle démocratique.

Il considère ainsi que « ces géants de l'Internet sont les seules entreprises de l'histoire à être parvenues à ce que leur production échappe en grande partie à toute réglementation. Ils dominent ainsi les marchés, sont extrêmement rentables en Bourse et influencent largement l'opinion publique et la politique, tout en restant très populaires du grand public. Ce contexte de concentration du pouvoir, l'absence de réglementation du secteur des logiciels et des services Internet, et l'histoire de la réglementation juridique des technologies doivent éclairer le débat actuel sur l'éthique et les lois relatives à l'IA ».

Ainsi, « l'absence de cadre constitutionnel a entraîné un mépris largement généralisé de la loi et mis la démocratie en danger, comme en témoigne le récent scandale Facebook – Cambridge Analytica ».

Face au pouvoir des données et aux dangers qu'il représente, allons plus loin que le RGPD

À ce stade, et bien que le recul d'une grosse année de mise en œuvre reste insuffisant pour tirer de l'application du RGPD des conclusions définitives, il apparaît que la nouvelle réglementation ne suffira pas à faire face aux deux principales menaces que font le peser les GAFA sur nos vies :

- l'accumulation de données personnelles, appréhendées comme une nouvelle forme de capital, leur donne un niveau de pouvoir et une force de frappe économique inédite, bien au-delà de ce que pouvaient représenter les grands trusts à la fin du XIX^{e} siècle avant le « Sherman Act » ;
- le traitement massif de ces données personnelles, notamment au moyen de procédés d'intelligence artificielle, permet de manipuler des segments entiers de l'opinion et fait peser un risque énorme sur la démocratie.

Si elles souhaitent reprendre le dessus, les grandes démocraties devront inévitablement aller bien plus loin que le RGPD, qui n'est finalement qu'une tentative – plus ou moins réussie – de protection de la vie privée des personnes mais ne règle en rien la question du pouvoir politique et économique lié à l'accumulation des données par les GAFA, ni celle du danger que l'usage de ces données fait peser sur la démocratie.

Les débats sont d'ailleurs en train de se déplacer sur le terrain du statut juridique des données. On voit apparaître une nouvelle ligne de fracture, témoignant, en creux, de l'insuffisance du RGPD. D'un côté, certains prônent le principe de l'appropriation des données personnelles par les personnes concernées. Les données seraient ainsi la propriété privée des personnes qu'elles concernent, qu'elles pourraient revendre, ou, à l'inverse, protéger plus fortement. Il s'agirait de pousser plus radicalement la logique induite par le RGPD et la place prise par la notion de consentement préalable au traitement des données. D'un autre côté, la question de la création d'un statut de bien commun pour les données en réseau commence à émerger, s'appuyant notamment sur les travaux iconoclastes mais peut-être visionnaires d'Evgeni Morozov.

Finalement, la question de la domestication des GAFA et de l'encadrement de la matière première à l'origine de leur puissance réactive quelques vieux clivages nés au XIX^{e} siècle, où l'émergence du capitalisme industriel voyait déjà s'affronter les libéraux, garants des libertés individuelles, aux socialistes et collectivistes, cherchant à mettre le capital au service du bien commun.

Dans ce retour des grands débats de la fin du XIX^{e} siècle, n'oublions pas non plus cette proposition

d'Elizabeth Warren, qui suggère de démanteler les GAFA, sur le modèle des grandes lois antitrust du tournant des XIX^{e} et XX^{e} siècles.

Les présentes questions seront, peut-être, et contre toute attente, le terrain sur lequel va se jouer le retour de l'affrontement entre libéraux et régulationnistes, et, partant, d'une réactivation contemporaine du clivage droite/gauche.