ANNUAIRE FRANÇAIS DE RELATIONS INTERNATIONALES

2019

Volume XX

PUBLICATION COURONNÉE PAR

L'ACADÉMIE DES SCIENCES MORALES ET POLITIQUES

(Prix de la Fondation Edouard Bonnefous, 2008)

Université Panthéon-Assas
Centre Thucydide

PRIVACY VS VIE PRIVÉE

Le droit européen aux prises avec les GAFA

PAR

Roseline LETTERON (*)

L'acronyme GAFA désigne les entreprises identifiées comme les acteurs les plus puissants sur Internet, Google, Amazon, Facebook, Apple. *A priori*, ce rassemblement se caractérise d'abord par son hétérogénéité, car ces firmes ne semblent rien avoir de commun. Apple, la plus ancienne, créée en 1976, trouve son origine dans la création de l'ordinateur individuel et est la seule qui ne soit pas issue du Web. Amazon n'a rien inventé, mais pratique le e-commerce depuis 1994, aujourd'hui à une échelle mondiale. Facebook, née en 2004 comme réseau social, est aujourd'hui une régie publicitaire et une plateforme qui accueille toutes sortes de contenus. Google enfin, né en 1998 du moteur de recherches qui porte son nom, se présente désormais comme une galaxie d'entreprises intervenant dans des domaines aussi divers que la fourniture d'accès à Internet, la publicité, la fibre optique, la recherche en robotique et intelligence artificielle ou les fonds d'investissement. Toutes ses filiales sont gérées par une *holding*, Alphabet, créée en 2015 et dont le siège est à Mountain View en Californie. La liste des GAFA peut évidemment être allongée et certains y ajoutent Microsoft, usant alors de l'acronyme GAFAM. Cet élargissement n'apporte cependant pas d'éclairage particulier à une étude centrée sur la protection de la vie privée et qui sera donc limitée aux firmes se consacrant, au moins en partie, à la valorisation commerciale des données personnelles. Microsoft comme Apple ne sont donc pas directement concernés par l'analyse, dès lors que l'une commercialise des programmes et l'autre des matériels. Quoi qu'il en soit, la diversité de ces entreprises ne doit pas cacher l'importance de ce qui les rapproche, justifiant pleinement cette vision englobante portée par l'acronyme GAFA.

Leur premier point commun réside dans le fait qu'elles évoluent dans un marché mondialisé et que chacune d'entre elles constitue une énorme puissance financière. Pour la seule année 2017, les revenus de Facebook, les plus modestes du groupe, s'élevaient à plus 40 milliards de dollars,

(*) Professeur de Droit public à Sorbonne-Université (France).

alors que ceux d'Apple, les plus élevés, grimpaient à 229 milliards. Entre les deux, Amazon affichait presque 178 milliards de dollars de revenus et Google/Alphabet 111 milliards (1). Cette mondialisation des marchés ne signifie pas que ces entreprises soient dépourvues de lien de nationalité. Elles ont pour point commun d'être nées aux Etats-Unis et de relever du droit américain. Trois d'entre elles ont leur siège dans la Silicon Valley, en Californie (Facebook, Google, Apple), et Amazon est installée à Seattle dans l'Etat de Washington. Toutes utilisent le droit américain comme un bouclier juridique dans les combats qui les opposent au reste du monde, car leur puissance est telle qu'elles n'hésitent pas à prétendre se soustraire au droit interne des Etats dans lesquels elles interviennent, en particulier les Etats membres de l'Union européenne (UE).

Le second point commun entre les GAFA réside ainsi dans cette relation conflictuelle que ces firmes entretiennent avec le droit continental, tant celui de l'Union européenne que celui des Etats membres. Ces points de friction se déploient sur des terrains divers et le premier d'entre eux est sans doute le droit de la concurrence. C'est ainsi que Google a été condamné à deux reprises par l'Union européenne pour abus de position dominante, d'abord en juin 2017 à une amende de 2,42 milliards de dollars pour avoir favorisé son comparateur de prix « Google Shopping » dans la recherche en ligne, au détriment de services concurrents, puis, en juillet 2018, à une seconde amende de 4,3 milliards de dollars pour avoir assuré la suprématie de son moteur de recherche dans le système d'exploitation pour Smartphone, Android.

Un autre terrain de conflit se trouve dans la volonté des Etats de taxer le chiffre d'affaires de firmes qui développent leurs activités sans le support d'installations situées sur le territoire européen. Le droit applicable, repris dans la plupart des conventions fiscales, repose traditionnellement sur la notion d'« *établissement stable* », ce qui signifie que ne peut être imposée qu'une entreprise dotée d'un pouvoir de décision suffisamment indépendant de la *holding* pour l'engager dans une relation commerciale autonome. Utilisant habilement cette définition, les GAFA adoptent une tactique simple consistant à externaliser les activités de prestation, de sorte que la succursale européenne ne sera dotée que de moyens et de fonctions très limités et, par conséquent, ne pourra être qualifiée d'établissement stable (2). Devant une telle situation, une convention multilatérale a été signée sous l'égide de l'Organisation de coopération et de développement économiques (OCDE) le 7 juin 2017. Elle comporte un article 12 qui considère comme « *établissement stable* » toute entreprise qui « *conclut habituellement des contrats* », même de manière routinière, dès lors qu'ils engagent la *holding*. Le conflit est cependant loin d'être terminé, dès lors

(1) P. Boittiaux, « Les revenus mirobolants des GAFA », *Statista,* 2 fév. 2018, disponible sur le site Internet fr.statista.com/infographie/12778/les-revenus-mirobolants-des-gafam/.

(2) Par exemple, Tribunal administratif de Paris, *Société Google Ireland Limited*, D. IP/IT 2018, 12 juil. 2017, p. 68, n. Gutman.

que l'Irlande, principal abri des GAFA dans l'Union européenne en raison de son taux d'imposition très favorable, a émis des réserves sur l'article 12. L'idée d'une taxation spécifique des acteurs du numérique fait néanmoins son chemin.

Le point de friction essentiel entre les GAFA et le droit continental se trouve cependant dans le respect de la vie privée et de la protection des données personnelles. Le conflit avec Google suscite ainsi un intérêt qui va bien au-delà des cercles de l'expertise juridique pour prendre à témoin l'opinion publique. Contrairement au droit de la concurrence et au droit fiscal, la vie privée concerne en effet chaque individu. L'enjeu est alors bien différent, car les GAFA entendent mettre en œuvre un niveau de protection bien inférieur à celui qui s'est développé sur le territoire des Etats européens depuis le dernier quart du XX^{e} siècle. Refusant de se soumettre au droit européen, ils apparaissent comme le vecteur d'une pénétration du système juridique américain en Europe, son cheval de Troie, dans la mesure où ils s'efforcent d'imposer la définition américaine de la vie privée ainsi que son mode d'organisation fondé sur le *soft law*. Leurs ambitions rencontrent cependant des obstacles et ce combat autour de la vie privée incite à un renforcement du droit européen, dans le but de s'opposer à cette offensive du droit américain.

Les GAFA, cheval de troie du droit américain

Les revenus des GAFA, plus particulièrement de Google et Facebook, reposent largement sur l'exploitation commerciale des données personnelles de leurs clients. Si l'accès au service est gratuit, la firme exploite et revend des informations précieuses pour les annonceurs, car elles permettent d'établir des profils de comportement et de consommation. Une telle pratique n'a rien d'illicite au regard du droit américain, qui conçoit l'information comme un bien susceptible d'échanges commerciaux, ce qui est désormais admis par le droit européen incarné dans le règlement général sur la protection des données (RGPD) du 27 avril 2016, en vigueur depuis le 25 mai 2018 (3). La différence réside cependant dans le choix américain de faire prévaloir cette vision très libérale de la liberté d'information sur le droit au respect de la vie privée. Cette dernière n'est l'objet que d'une protection de basse intensité, organisée par des règles de bonnes pratiques ou des instruments techniques incorporés au système.

Libre circulation de l'information v. vie privée

Les Pères fondateurs ont envisagé la liberté de l'information en réaction à un héritage britannique dont ils avaient eu à souffrir. L'Angleterre du XVII^{e} siècle pratiquait en effet, jusqu'en 1694, la censure préventive des écrits et de la presse. Une infraction de diffamation séditieuse interdisait en

(3) Règlement (UE) 2016/679 du 27 avril 2016, *Journal officiel*, n°L119/1, 4 mai 2016.

outre de critiquer les pouvoirs publics et le gouvernement. Dès la première moitié du XVIII[e] siècle, avant même la Déclaration d'indépendance, le droit américain affirmait sa différence dans le retentissant procès Zenger en 1735, acquittant le propriétaire du *New York Weekly Journal*, accusé d'avoir précisément dénigré le gouverneur de la Colonie de New York (4). Après l'indépendance, le premier amendement venait pérenniser cette conception libérale de la liberté d'expression en affirmant que « *le Congrès ne fera aucune loi* [...] *qui restreigne la liberté d'expression, ou celle de la presse* ». Il est vrai que la tentation de limiter la liberté d'expression n'a pas toujours été absente aux Etats-Unis, du *Sedition Act* de 1798 à *l'Espionage Act* de 1917 et jusqu'au *Smith Act* de 1940, qui fut le fondement juridique des poursuites du maccarthysme. En revanche, il est désormais acquis, depuis la décision *Reno v. American Civil Liberties Union* (ACLU) de 1997 que l'expression sur Internet est protégée par le premier amendement au même titre que n'importe quel autre support d'information (5).

Il est surtout remarquable qu'aucune disposition du droit américain n'ait jamais sérieusement limité la liberté de faire circuler l'information, de l'acheter et de la vendre. Ce libéralisme, cette fois purement économique, est certainement l'un des facteurs ayant permis le considérable développement des GAFA. Ces entreprises revendiquent une mondialisation des flux d'informations, lesquels, selon elles, doivent circuler librement, sans considération de frontières et donc sans entrave provenant du droit des Etats dans lesquels transitent ces données ou résident leurs clients.

Cette revendication est d'autant plus aisément formulée que la vie privée n'est pas mentionnée dans les amendements à la Constitution qui constituent le *Bill of Rights* américain. Elle n'est pas davantage consacrée par une grande loi et est le produit d'une construction doctrinale initiée dans l'article « The right to privacy », rédigé par Samuel Warren et Louis Brandeis dans la *Harvard Law Review* en 1890 (6). C'est seulement en 1960 que William Prosser identifie quatre atteintes possibles à la *privacy* : l'ingérence dans les affaires privées de la personne, la divulgation publique de faits privés, la publicité diffamatoire et l'appropriation du nom d'une personne (7). Enfin, en 1970, Alan Westin propose d'ajouter à cette liste la protection des données personnelles, dans son ouvrage *Privacy and Freedom* (8). La protection des données personnelles n'est donc qu'un élément de la vie privée, qui elle-même ne donne pas lieu à une législation spécifique. Elle n'est protégée par les tribunaux américains que sur le

(4) M. Cucheval Clarigny, « La presse au XIX[e] siècle. La presse aux Etats-Unis », *Revue des Deux Mondes*, t. 3, 1853, pp. 447 et suiv.

(5) Cour Suprême, *Reno v. ACLU*, 521 U.S. 844, 26 juin 1997.

(6) S. Warren / L. Brandeis, « The right to privacy », *Harvard Law Review*, vol. IV, 15 déc. 1890, disponible à l'adresse faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

(7) W. Prosser, « Privacy », *California Law Review*, vol. XLIII, n°3, août 1960, pp. 383 et suiv.

(8) A. Westin, *Privacy and Freedom*, Bodley Head, 1970, 487 p.

fondement d'une responsabilité civile et sans remettre en cause le principe de la libre circulation de l'information.

La situation est bien différente sur le territoire européen, particulièrement en France. La vie privée apparaît aussi au XIX^e^ siècle, non pas dans des écrits doctrinaux mais dans une décision du tribunal civil de la Seine qui, en 1858, sanctionne la publication dans un journal de la photographie de la comédienne Rachel sur son lit de mort (9). La vie privée devient très rapidement un élément de l'ordre public, avec la loi du 11 mai 1868 qui punit d'une contravention la publication dans un périodique d'un « *fait de la vie privée* ». Un siècle plus tard, le droit au respect de la vie privée est consacré comme liberté publique par la loi du 17 juillet 1970 qui introduit dans le code civil un article 9 ainsi rédigé : « *Chacun a droit au respect de sa vie privée* », tout manquement étant constitutif d'un délit. Le Conseil constitutionnel lui confère enfin valeur constitutionnelle dans une décision du 23 juillet 1999, en le considérant comme une « *liberté individuelle* » au sens de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 (10).

La protection des données personnelles s'intègre naturellement dans ce mouvement. Elle est consacrée comme une liberté dès la célèbre loi du 6 janvier 1978 qui affirme que « *l'informatique doit être au service de chaque citoyen* [...]. *Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* » (11). Ce texte a eu une influence considérable sur l'émergence du droit européen de la protection des données, concrétisée d'abord par la directive du 24 octobre 1995 (12) à laquelle a succédé le règlement général sur la protection des données (RGPD) du 27 avril 2016 (13). Un droit de la protection des données est ainsi mis en œuvre, qui a vocation à s'appliquer sur l'ensemble du territoire des Etats membres de l'Union européenne, y compris bien entendu aux opérateurs étrangers que sont les GAFA.

Bonnes pratiques v. règle de droit

A cette différence dans la définition même de la vie privée et de la protection des données correspond une autre distinction liée aux mécanismes de garantie. Le droit européen repose sur la double intervention d'une autorité de contrôle indépendante généralement dotée d'un pouvoir de sanction, à laquelle vient s'ajouter une garantie juridictionnelle. Sous l'empire de la directive de 1995, plus précisément sur le fondement de son article 29, les institutions chargées de la protection des données dans les

(9) Tribunal civil de la Seine, *Felix c. O'Connell*, D. P. 1858 III, 62, 18 juin 1858.

(10) Conseil constitutionnel, déc. n°99-416 du 23 juillet 1999, *LPA*, 20 oct. 1999, p. 23, n. Mathieu.

(11) Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *Journal officiel*, 7 janv. 1978, p. 227.

(12) Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, *Journal officiel*, n°L 281, 23 nov. 1995, pp. 31 et suiv.

(13) Règlement (UE) 2016/679 du 27 avril 2016, *op. cit*.

Etats de l'UE étaient déjà regroupées au sein du « G29 », « *groupe consultatif et indépendant* » chargé notamment de donner un avis sur le niveau de protection dans la Communauté « *et dans les pays tiers* ».

La Commission nationale de l'informatique et des libertés (CNIL) française a ainsi été chargée de gérer, au nom du G29, le contentieux avec Google sur la protection des données.

Tel qu'il est apparu, ce différend met en lumière les instruments juridiques et techniques employés par les GAFA pour se soustraire au droit européen. Ils ont connu une évolution assez sensible et les règles de confidentialité de Google ont ainsi été modifiées vingt-sept fois de juin 1999 à novembre 2018 (14). Dans un premier temps, en 1999, Google se déclare seulement « *sensible aux préoccupations* » de ses abonnés et annonce une politique de transparence en ce domaine. En 2012, la situation n'a guère évolué et Google produit une « *charte d'auto-régulation* », ce qui signifie que l'entreprise accepte de respecter les règles qu'elle a elle-même édictées. Sur le fond, elle explique qu'elle collecte effectivement des données personnelles, y compris celles de localisation, dans le but de proposer à l'internaute des « *contenus adaptés* », c'est-à-dire des messages publicitaires établis en fonction d'un profil établi grâce à l'intelligence artificielle. Les « *règles de confidentialité* » actuellement en vigueur et datées de mai 2018 ne modifient pas sensiblement l'approche de 2012.

Aux yeux des GAFA, en particulier de Google, les règles de bonne pratique sont suffisantes pour assurer la protection de la vie privée. Les entreprises s'appuient ainsi sur la « *Privacy by Design* », principe qui impose de protéger la vie privée dès la conception d'un système informatisé, d'anticiper les risques de divulgation et de prendre les mesures de protection adéquates. Cette démarche n'est pas dépourvue d'arrière-pensées commerciales car, au-delà de la protection des données personnelles, elle a aussi pour objet d'accroître la confiance des utilisateurs et donc d'obtenir un avantage compétitif (15). La simplicité de ce mécanisme d'auto-régulation n'est toutefois qu'apparente. L'efficacité de la « *Privacy by Design* » n'est pas démontrée dans le cas du « *big data* », technique d'exploitation de l'immense masse des données circulant sur Internet dans un but de modéliser les opinions des internautes ou leurs habitudes de consommation. Utilisant l'intelligence artificielle, les systèmes auto-apprenants collectent ainsi des données dans des fichiers qui n'ont fait l'objet d'aucune protection, même dans le cadre de la « *Privacy by Design* ». En l'état actuel des choses, la « *Privacy by Design* » ne semble pas étendue à l'infrastructure même des réseaux ni à l'ensemble des objets connectés.

Le droit européen ne rejette pas la « *Privacy by Design* ». Le RGPD, dans son article 25, impose aux responsables des traitements de prendre

(14) Les archives de ces règles sont publiées sur le site policies.google.com/privacy/archive.

(15) M. Dary / L. Benaissa, « *Privacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre », *D. IP/IT*, 2016, p. 476.

des mesures dès leur création pour les assortir des garanties nécessaires à la protection des données. Cette référence à un code de conduite ou à une auto-régulation n'est cependant conçue que comme le complément d'une législation contraignante qui repose sur un certain nombre de principes contraignants, parmi lesquels le droit à l'oubli et le principe du consentement exprès de l'internaute à la collecte et à l'exploitation de ses données personnelles. Ces droits de l'internaute sont précisément au cœur du conflit avec les GAFA, qui tentent de se soustraire aux obligations qu'ils imposent.

Un droit européen mieux armé

Le règlement général de protection des données (RGPD), en vigueur sur l'ensemble du territoire de l'Union européenne depuis le 25 mai 2018, constitue aujourd'hui l'instrument essentiel de la réaction européenne face aux violations de la vie privée commises par les GAFA. Il a pour objet de renforcer l'efficacité de l'action européenne, grâce à deux instruments essentiels. Le premier vise à une meilleure réactivité du droit européen. Le système du G29, dans lequel une autorité de contrôle d'un Etat membre recevait un mandat d'agir au nom de la Commission, cède désormais la place à une formule dans laquelle chaque autorité de contrôle des Etats membres est directement chargée de la mise en place du RGPD. Le second instrument d'efficacité réside plus simplement dans un renforcement des sanctions financières, afin de les rendre plus dissuasives lorsqu'elles sont infligées aux puissances que sont les GAFA. Conditionnées par l'existence d'un réel contrôle préalable exercé par l'autorité de contrôle, elles vont du simple rappel à l'ordre à une sanction pécuniaire susceptible d'atteindre dix millions d'euros ou 2% du chiffre d'affaires de l'entreprise, précisément lorsqu'une atteinte aux droits des personnes est constatée. En cas de refus de se plier à une injonction de l'autorité de contrôle, le plafond de la sanction peut être porté à vingt millions d'euros ou 4% du chiffre d'affaires. A cela s'ajoute, dans le cadre de la loi française du 21 juin 2018, une éventuelle astreinte de 100 000 € par jour si le traitement n'est pas rapidement mis en conformité au RGPD (16).

Cet arsenal juridique est de nature à renforcer la crédibilité des instances de contrôle européennes, plus précisément de la CNIL. On doit en effet se souvenir qu'en 2014, cette dernière n'avait pu condamner Google qu'à une amende de 150 000 € pour avoir refusé de donner à ses utilisateurs une information sur les finalités et l'ampleur de la collecte de leurs données personnelles et, surtout, pour ne pas avoir réellement sollicité leur

(16) Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles, *Journal officiel*, n°0141, 21 juin 2018, texte n°1.

consentement (17). A l'époque, une agence spécialisée dans le référencement évaluait toutefois, pour l'année 2013, les revenus publicitaires de Google en France à plus de 1 400 000 € (18).

Ce renforcement du droit par le RGPD, certes spectaculaire, n'a toutefois rien d'inattendu. Le contentieux entre l'Union européenne et les GAFA se trouve directement à l'origine de cette volonté de durcir les textes et de renforcer les moyens des autorités chargées de les appliquer. Il s'est cristallisé autour de deux principes fondamentaux que ces firmes se montrent réticentes à appliquer : le droit à l'oubli et le consentement éclairé de la personne.

Droit à l'oubli numérique

Inspiré du droit de la presse, le droit à l'oubli permet de sanctionner et de réparer les révélations sur le passé d'une personne, passé qui relève de sa vie privée. Le droit à l'oubli est apparu pour sanctionner les révélations sur le passé judiciaire d'une personne qui a jadis été condamnée, qui a purgé sa peine et qui revendique donc le droit d'être oubliée. Sur Internet, il se traduit aujourd'hui par la mise en œuvre d'un droit d'effacer ses traces, plus précisément d'un droit au déréférencement. Ce dernier a toutefois une portée plus étendue que le droit à l'oubli : il ne concerne pas seulement la protection de la vie privée, mais permet aussi de supprimer des données portant atteinte à d'autres intérêts, par exemple le droit d'auteur. Considéré ainsi, le droit à l'oubli peut être considéré comme un élément du droit au déréférencement, spécifiquement tourné vers la protection de la vie privée.

La première affaire notable de revendication du droit à l'oubli est celle initiée par Max Mosley, au début des années 2000. Elle a connu un certain retentissement, à la fois par la personnalité de l'intéressé, ancien président de la Fédération internationale du sport automobile, et par la multiplication des recours qu'il a introduits devant plusieurs juges européens. Il se plaignait d'une atteinte au droit à l'oubli, certains mots-clefs utilisés sur Google faisant apparaître des photographies le montrant dans des postures très intimes, clichés provenant d'un *tabloïd* britannique. Dès lors qu'ils étaient accessibles *via* Google.fr, il s'est adressé au tribunal de grande instance de Paris. En 2008, il a obtenu un référé ordonnant à Google le retrait des images, mais la société s'est bornée à répondre, dans un bref communiqué, qu'il ne lui appartenait pas de « *faire la police sur Internet* ». La firme affirmait alors que le rôle d'un moteur de recherches était de permettre la libre circulation des données, sans avoir à intervenir sur les contenus indexés. Le 6 novembre 2013, le tribunal de grande instance (TGI) de Paris a donc rendu un jugement au fond, exigeant de

(17) CNIL, Délibération n°2013-420 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société *Google Inc*, commentaire X. Berne, *NextINpact*, 9 janv. 2014, disponible à l'adresse www.nextinpact.com/news/85283-pourquoi-cnil-a-inflige-amende-150-000-euros-a-google.htm.

(18) B. Ferran, « Plus d'un milliard d'euros de revenus pour Google en France », *Le Figaro*, 18 déc. 2014.

Google le retrait des photos pendant une durée de cinq ans et assortissant l'injonction d'une astreinte de 1 000 € par jour.

A l'époque, la réaction des juges français était apparue peu efficace et isolée. L'inefficacité est évidente si on considère que le juge ne pouvait infliger la moindre sanction à Google, l'injonction étant seulement assortie d'une astreinte d'un montant dérisoire. L'isolement est aussi une réalité, car aucune position européenne commune n'existait alors. Certes, Max Mosley avait obtenu l'interdiction de la diffusion des images litigieuses de la High Court of Justice de Londres, mais la Cour européenne des droits de l'homme, dans un arrêt du 10 mai 2011, avait estimé que la publication dans le *tabloïd* ne portait pas une atteinte excessive à la vie privée de l'intéressé, affirmant qu'elle participait au débat d'intérêt général (19). Certes, la Cour européenne n'applique pas le droit de l'Union européenne, mais sa décision témoigne d'un certain pouvoir d'attraction de la conception américaine de la liberté d'expression, qui fait prévaloir la liberté d'information sur la vie privée des personnes. A cet égard, cette jurisprudence a certainement nui à la construction d'un droit à l'oubli européen en le rendant peu intelligible. Pourquoi en effet contraindre Google à déréférencer une information dont la divulgation dans la presse a été jugée licite par un autre juge européen ?

C'est finalement la Cour de justice de l'Union européenne (CJUE) qui est intervenue pour consacrer le droit à l'oubli sur Internet, dans sa célèbre décision *Google Spain SL* du 13 mai 2014 (20). Le requérant se plaignait qu'une recherche portant sur son nom dans Google.es faisait mention d'une vente de ses biens sur saisie judiciaire, une quinzaine d'années auparavant. A l'époque, le texte européen applicable est la directive de 1995 qui énonce que les données personnelles conservées devaient être « *exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes* [...] *soient effacées ou rectifiées* » (21). Cette décision a permis de développer un standard européen dans ce domaine. Les juges internes se sont saisis de cette jurisprudence et ont usé de leur pouvoir d'injonction pour ordonner à Google de déréférencer des données personnelles dont la diffusion actuelle portait atteinte au droit à l'oubli (22). La Cour de cassation française, dans une décision du 12 mai 2016, évoque à son tour un « *droit à l'oubli numérique* » pour justifier la demande de deux requérants visant la désindexation de leur nom des archives numériques d'un journal (23). Avec cette décision, les juges internes français se donnaient les moyens de lutter plus efficacement

(19) Cour européenne des droits de l'homme (CEDH), 10 mai 2011, *Mosley c. Royaume-Uni*, req. N°48009/08 ; D. Fenasse, « Le droit au respect de la vie privée s'efface devant la liberté d'expression », *LegalNews*, 14 juin 2017.

(20) CJUE, 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Espanola de Proteccion de Datos (AEPD) et Maria Costeja Gonzalez*, C-131/12, *AJDA*, 2014, p. 1147, chr. Aubert, Broussy, Cassagnabère.

(21) Art. 6 de la directive du 24 octobre 1995, *Journal officiel*, n°L 281, 23 nov. 1995, p. 31.

(22) Par exemple, TGI Paris, ord. référé, 19 décembre 2014, *Marie-France M. c. Google France et Google Inc*. *Legalis*, 9 janv. 2015.

(23) Cour de cassation, Chambre civile, 1re Chambre, 12 mai 2016, pourvoi n°15-17729.

contre les agissements des GAFA en matière de collecte et de conservation des données personnelles.

Le RGPD définit désormais un standard européen dans ce domaine. Son préambule énonce que « *les personnes concernées devraient avoir le droit de faire rectifier des données à caractère personnel les concernant, et de disposer d'un droit à l'oubli* » (24). Son article 7 garantit donc un « *droit à l'effacement ('droit à l'oubli')* » qui impose aux entreprises de traiter les demandes « *dans les meilleurs délais* ».

Le moteur de recherches de Google est évidemment au cœur de la revendication du droit à l'oubli et la firme s'efforce, autant que possible, de se soustraire aux exigences européennes. Elle utilise pour cela deux méthodes principales : d'une part, le recours à un pouvoir discrétionnaire de décider ce qui doit être rendu inaccessible ; d'autre part, l'utilisation habile de la diversité de ses moteurs pour offrir d'autres accès aux informations déréférencées.

Après l'arrêt *Google Spain* et surtout l'entrée en vigueur du RGPD, il n'était plus possible d'invoquer l'inapplicabilité du droit européen à une entreprise américaine. Google a donc choisi de se plier, au moins en apparence, à ses prescriptions. Les internautes peuvent désormais accéder à un formulaire spécifique de déréférencement ou « *demande de suppression d'informations personnelles* » (25). Google affiche en temps réel sur une page spécifique le nombre de demandes de suppression (747 899 au 25 novembre 2018) et le nombre de pages faisant l'objet de ces demandes (2 863 726). On y apprend également que, à la même date, Google a accepté 56% des déréférencements, ce qui signifie qu'il en a aussi rejeté 44% (26). Derrière cette apparente transparence, se cache en réalité une grande opacité, car les critères mis en œuvre par Google pour accepter ou rejeter la demande demeurent largement inconnus.

D'une manière générale, la firme semble toujours réticente à l'égard d'un système qui lui impose de contrôler les contenus qu'elle rend accessibles. En outre, l'idée d'offrir aux particuliers une telle prérogative va directement à l'encontre d'une tradition américaine qui repose sur la libre circulation de l'information, à laquelle seul un juge peut poser des limites (27). Cette réticence explique largement une pratique plus brutale qui consiste à ne rendre accessible l'information que sur le moteur à partir duquel l'internaute formule sa demande. Une donnée personnelle d'un internaute français déréférencée demeurera ainsi accessible à partir des mêmes mots-clefs si on utilise Google.com ou un autre nom de domaine européen Google.fr, .de, .it, etc. La firme justifie cette pratique par l'existence d'un « *territoire réputationnel* », notion qui repose sur l'idée que

(24) Al. 65 du Préambule du RGPD, précité.

(25) *Cf.* le site Internet www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=636787671256366227-553481907&rd=1&pli=1.

(26) *Cf.* le site Internet transparencyreport.google.com/eu-privacy/overview.

(27) I. Falque-Perrotin, « Pour un droit au déréférencement mondial », *Le Monde*, 29 déc. 2016.

la visibilité d'une personne est limitée à ceux qui habitent dans la même région. On peut ainsi s'étonner de voir une entreprise qui revendique une liberté d'information mondialisée réduire en même temps la vie privée d'une personne à son espace vernaculaire.

Pour le moment, la jurisprudence européenne est loin d'être fixée dans ce domaine et les incertitudes du Conseil d'Etat français en témoignent. Depuis un arrêt du 19 juillet 2017, ce dernier considère que la CNIL est compétente pour traiter des demandes de déréférencement adressées au moteur de recherches Google qui doit être considéré comme « *un traitement de données à caractère personnel unique* », quel que soit le nom de domaine utilisé par l'internaute pour faire sa recherche. Il ajoute, non sans malice, que Google lui-même admet cette unité du moteur de recherche, puisque toute consultation, d'où qu'elle vienne, donne lieu à une redirection automatique des témoins de connexion (« *cookies* ») vers les autres extensions (28). En revanche, le Conseil d'Etat pose une question préjudicielle à la Cour de justice de l'Union européenne sur la manière dont doit être interprété le droit au référencement au regard du RGPD. S'il est étendu à l'ensemble des noms de domaine gérés par le moteur de recherches, la difficulté réside dans le fait qu'il concernera aussi des Etats non membres de l'UE. Cette forme d'extra-territorialité du règlement européen serait toutefois le seul moyen de garantir l'effectivité du droit à l'oubli. Ces questions préjudicielles montrent que le RGPD est loin d'avoir entièrement résolu la question du droit à l'oubli et que les GAFA exploitent avec beaucoup d'habilité les failles du dispositif. Il en est de même en matière de consentement de la personne à la collecte, la conservation et l'exploitation de ses données personnelles.

Consentement de la personne

Le consentement est défini par le RGPD comme une « *manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte* [...] *que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Le texte européen renforce donc les obligations des responsables de traitements en leur imposant de formuler de manière compréhensible les demandes de consentement, ce dernier pouvant par ailleurs être retiré à tout moment. Aux yeux des GAFA, une telle exigence est pratiquement inacceptable, car elle conduit à remettre en cause la pratique du « Big Data » qui connaît actuellement un développement considérable et qui, au regard du droit américain, est parfaitement licite. Elle consiste à exploiter l'immense masse de données circulant sur Internet, y compris les données personnelles, dans le but de connaître les opinions des internautes, leurs habitudes de consommation, etc. La modélisation de ces informations, renforcée par le recours à l'intelligence artificielle, permet

(28) Conseil d'Etat, 19 juillet 2017, *Google Inc*. req. n°399922, *Revue trimestrielle de droit européene*, 2018, p. 396, n. Bouveresse.

de mettre en place des systèmes de profilage particulièrement efficaces en matière de marketing commercial, voire de marketing politique.

Les relations entre Facebook et Cambridge Analytica illustrent parfaitement cette tension entre une entreprise américaine dont l'activité principale est la valorisation des données personnelles des internautes et un droit européen qui repose sur le principe de protection des données et prohibe formellement tout profilage sans le consentement de la personne concernée.

Entre 2013 et 2014, 87 millions d'utilisateurs de Facebook dans le monde, parmi lesquels bon nombre d'Européens, dont environ 200 000 Français, ont téléchargé une application développée par Cambridge Analytica, entreprise aujourd'hui déclarée en faillite, dont le siège était situé à Londres. S'abritant derrière une finalité de recherche académique exigeant des réponses à un questionnaire, le logiciel siphonnait, à l'insu des intéressés, les données personnelles présentes dans leur compte Facebook ainsi que celle de leurs « amis ». Ces données étaient ensuite analysées et revendues pour être utilisées pour des campagnes politiques, en particulier celle de Donald Trump en 2016 (29). Le principe du consentement éclairé, exigé en droit européen, a été totalement ignoré, les victimes n'ayant même jamais été informées de la finalité réelle de l'opération. L'étude des garanties de confidentialité affichées par Facebook montre que la firme se borne à expliquer « *comment la plateforme Facebook procède pour protéger sa communauté* ». Elle privilégie la « *Privacy by Design* », sans d'ailleurs en préciser les principes, ignorant l'obligation de consentement imposée par le droit européen.

Loin d'être close, l'affaire Cambridge Analytica suscite actuellement plusieurs séries de réactions. Aux Etats-Unis d'abord, Mark Zuckerberg a été contraint de s'expliquer et, surtout, de présenter des excuses publiques devant différentes institutions, dont le Congrès. Au Royaume-Uni, l'Information Commissioner's Office, équivalent britannique de la CNIL, a lancé une enquête et remis un rapport au Parlement le 6 novembre 2018, constatant que Facebook avait commis de graves manquements aux principes de protection des données. Une amende de 500 000 £ a été infligée à l'entreprise (30). Dans l'Union européenne enfin, le Parlement européen a décidé, le 25 octobre 2018, de procéder à un audit portant sur la manière dont Facebook protège ou non les données personnelles de ses utilisateurs (31). De son côté, la Commission réfléchit activement aux

(29) M. Untersinger, « Comment une entreprise proche de Trump a siphonné les données de millions d'utilisateurs de Facebook », *Le Monde Pixel*, 18 mars 2018.

(30) ICO, *Investigation into the use of data analytics in political campaigns. A report to Parliament*, 6 nov. 2018, disponible à l'adresse ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

(31) Parlement européen, Résolution 2018/2855 RSP du 25 octobre 2018 sur l'exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données, disponible à l'adresse www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0433+0+DOC+PDF+V0//FR.

moyens à mettre en œuvre pour empêcher certaines firmes d'influencer les électeurs lors des élections européennes de 2019 (32).

L'affaire Cambridge Analytica illustre l'importance du contentieux entre les GAFA et le droit européen. Elle témoigne aussi d'une réelle volonté à la fois des Etats membres et de l'Union de renforcer les instruments juridiques susceptibles de contraindre ces firmes à respecter les principes de la protection des données personnelles.

Le renforcement actuel du droit européen est incontestable, mais la bataille est loin d'être gagnée. De leur côté, les GAFA s'efforcent en effet de construire une sorte de glacis juridique leur permettant de se mettre à l'abri des contraintes du droit européen et du droit des Etats membres de l'Union européenne.

De la même manière que la notion d'« établissement stable » est utilisée par Google pour échapper à la fiscalité française, celle d'« établissement principal » lui offre le moyen de se soustraire aux règles de la protection des données. Dans les mois qui ont suivi la décision Google Spain, les juges français admettaient en effet les requêtes en déréférencement dirigées contre Google France, filiale de Google Inc., alors même que cette filiale n'avait pas d'autre mission que d'acheter et de vendre de l'espace publicitaire et n'exerçait aucune responsabilité dans la gestion du moteur de recherches (33). L'idée était d'engager la responsabilité financière de Google à travers ses filiales présentes sur le territoire, principe permettant d'utiliser à leur encontre les voies d'exécution prévues par le droit interne. Cependant, dès décembre 2014, la jurisprudence française a évolué et les juges du fond ont considéré que seul l'entreprise-mère, à l'époque Google Inc., pouvait être considérée comme responsable du traitement au sens du droit français (34). Dès 2015, Google a largement élargi cette brèche, en multipliant les filiales autour d'une nouvelle Holding Alphabet, dans le but de mettre à l'abri du droit européen les activités les plus consommatrices de données personnelles et d'intelligence artificielle.

Dans cette bataille visant à échapper au droit continental, les GAFA sont aidés par l'administration américaine. Elle aussi considère que les données personnelles, y compris celles des Européens, sont des biens susceptibles d'échanges et d'appropriation, non seulement pour des motifs commerciaux mais aussi pour des considérations de sécurité.

Ses premiers efforts ont consisté à contourner la jurisprudence « *Digital Rights* » de la Cour de justice de l'Union européenne. Dans cette décision du 6 octobre 2016, la Cour de justice de l'Union européenne (CJUE) a en effet remis en cause l'accord autorisant les transferts massifs de données

(32) J. Bergounhoux, « L'UE pourrait sanctionner les partis politiques abusant des données des électeurs », *L'Usine digitale*, 27 août 2018.

(33) TGI, ord. référé, 16 septembre 2014, *M. et Mme X. et M. Y. c. Google France*, *Legalis*, 24 sept. 2014.

(34) TGI, ord. référé, 9 décembre 2014, *Marie-France M. c. Google France et Google Inc, Legalis*, 9 janv. 2015.

personnelles de l'Union européenne vers les Etats-Unis (35). Le recours était le produit d'un contentieux opposant un ressortissant autrichien qui contestait les transferts de ses données personnelles de Facebook Irlande (siège européen de l'entreprise) vers Facebook Etats-Unis. L'ancienne directive de 1995 admettait de telles pratiques d'exportation de données personnelles, à la condition toutefois, selon son article 25, que le pays tiers soit considéré comme exerçant à leur égard un « niveau de protection adéquat », c'est-à-dire équivalent de celui existant au sein de l'UE. En l'an 2000, un accord dit « Safe Harbor » entre le Département américain du Commerce et la Commission européenne avait suscité une décision de la Commission déclarant effectivement que le niveau de protection des données par les Etats-Unis était « *adéquate* » (36). L'arrêt du 6 octobre 2016 détruisait cette construction, la CJUE estimant que les données personnelles des internautes européens n'étaient pas en sécurité, le système prévoyant un simple mécanisme d'auto-certification par lequel l'entreprise déclare respecter la « *Privacy by Design* ». Usant d'un *lobbying* important, les Etats-Unis ont obtenu, avant même l'intervention de l'arrêt « *Digital Rights* », un nouvel accord dit « *Privacy Shield* » qui, certes, accroît la transparence en prévoyant une publicité de la liste des entreprises ayant accepté cette auto-régulation, mais qui repose exactement sur le même principe d'auto-certification.

Le *Cloud Act* (*Clarifying Lawful Overseas Data Act*), quant à lui, a été promulgué le 23 mars 2018, quelques jours avant la publication du RGPD. Cette coïncidence n'est probablement pas un hasard, car il s'agit cette fois d'anticiper l'application et de contourner les contraintes de ce dernider. Le RGPD consolide la position européenne en interdisant de transférer les données des résidents européens en dehors de l'Union européenne, principe applicable évidemment lorsque le récipiendaire américain des données européennes ne bénéficie pas d'une autorisation acquise dans le cadre du « *Privacy Shield* », par exemple lorsqu'il s'agit d'agences publiques. La loi du 20 juin 2018 adaptant le droit français au RGPD punit ainsi ce type de transfert de cinq ans d'emprisonnement et 300 000 € d'amende (37). Faute de pouvoir transférer les données, le gouvernement américain a donc entrepris d'aller les chercher directement dans les *clouds* utilisés par les internautes à des fins de sauvegarde et de conservation. C'est précisément l'objet du *Cloud Act*, qui repose sur la volonté des autorités américaines de se constituer un « *grenier à données personnelles* » (38). Considérées sous cet angle, les activités des GAFA sont utilisées comme une sorte de paravent permettant à l'administration américaine d'avoir

(35) CJUE, 6 octobre 2015, *M. Schrems c. Data Protection Commissioner, Digital Rights Ireland Ltd*, C-362/14.

(36) Décision de la Commission du 26 juillet 2000, C (2000) 2441, disponible à l'adresse eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32000D0520&from=FR.

(37) Loi n°2018-393 du 20 juin 2018 relative à la protection des données personnelles, *Journal officiel*, 21 juin 2018, texte n°1.

(38) E. Lamer, « Pourquoi le 'Cloud Act' américain inquiète l'Union européenne », *Le Soir,* 7 mars 2018.

accès aux données des internautes européens. Ces pratiques sont bien éloignées de la communication officielle des GAFA, lesquels se présentent volontiers comme les protecteurs des données personnelles de leurs clients ou abonnés face à une administration américaine intrusive. Il apparaît ainsi que la politique des Etats-Unis visant à la fois à exploiter les données personnelles à des fins commerciales et à les contrôler à des fins politiques ou de sécurité ne s'exerce pas contre les GAFA mais bien davantage avec leur accord, voire leur complicité.