Les cafés de la statistique

"La statistique éclaire-t-elle les questions de société" ?

Soirée du 20 juin 2018

Droit des données : où va-t-on ?

Introduction aux débats[1]

Les textes de droit importants sur les données se sont succédé de façon rapide ces dernières années, le plus connu étant le règlement européen de protection des données (RGPD) récemment entré en application. Et on annonce un nouveau texte dans un proche avenir : le règlement européen "e-privacy". Y a-t-il une orientation principale de ce déferlement législatif, ou bien existe-t-il des philosophies différentes, voire opposées ? Au-delà des principes, est-ce que les mesures d'application suivent, et renforcent effectivement la protection des citoyens, qu'il s'agisse de l'usage de leurs données personnelles, ou des algorithmes intervenant dans leurs vies ? Le droit européen est-il suffisamment puissant pour être appliqué par les grands opérateurs mondiaux ? En fin de compte, peut-on espérer atteindre un équilibre entre les nécessités du déploiement du progrès technique et la protection des individus et des sociétés ?

Invitée :
Judith Rochfeld
Professeur des universités
Directrice du Master 2 "Droit du commerce électronique et de l'économie numérique" à l'Université Panthéon-Sorbonne

Exposé introductif :

Le règlement général sur la protection des données (RGPD) est un règlement européen, adopté le 27 avril 2016 et effectivement mis en œuvre depuis le 25 mai 2018. Il est donc d'actualité et se télescope avec une autre affaire, celle dite de « Cambridge Analytica ». Facebook a en effet proposé à certains de ses utilisateurs, principalement aux États-Unis d'utiliser une application pour effectuer un test de personnalité. Ceux qui ont fait ce test n'étaient cependant pas conscients que cela permettait aux opérateurs de cette application d'avoir accès aux « like », donc aux comportements, appétences et centres d'intérêt, non seulement des personnes qui avaient répondu au test, mais de tous leurs « amis » qui s'étaient manifestés. On est donc passé de quelques milliers de personnes ayant effectué le test de personnalité à plusieurs dizaines de millions de personnes pour lesquelles une

[1] Tant l'exposé liminaire que le contenu des échanges sont structurés en quelques thèmes, sans suivre l'ordre chronologique. Par ailleurs, l'identité des intervenants n'était pas toujours connue et l'on a choisi de ne pas attribuer nominativement les propos. Au reste, ceux-ci ont été reconstitués à partir des notes du secrétariat sans reprendre leur formulation détaillée. Pour retracer le débat, les thèmes sont souvent introduits sous forme d'une question : ce qui vient ensuite n'est pas la seule réponse de l'invité, mais l'ensemble des contributions des participants

analyse menée au Royaume-Uni (transfert transatlantique) par la société Cambridge Analytica a permis de savoir si elles étaient plutôt prêtes à voter Donald Trump ou Hillary Clinton. Les premiers ont été particulièrement ciblés par des messages les incitant à voter pour Donald Trump. L'élection s'étant jouée, dans certains États à quelques dizaines de milliers de voix, on peut en conséquence réaliser que l'élection américaine a été fortement influencée par cette opération.

Le même soupçon pèse d'ailleurs sur le résultat des élections de 2015 au Nigeria ou sur l'issue du référendum du Brexit.

Au-delà de la publicité commerciale ciblée, on découvre donc que l'utilisation de données personnelles peut aussi jeter le doute sur l'issue de consultations politiques.

Das l'actualité récente, on peut également évoquer le site de rencontres à dominante homosexuelle Grindr, qui a lâché dans la nature des informations relatives à la vie sexuelle, à la séropositivité de ses utilisateurs. Il s'agit là d'une violation de sécurité, donc différente du cas Cambridge Analytica, mais qui illustre également un enjeu très important en termes de protection de la vie privée.

En face de ces immenses enjeux pour la démocratie, l'information et la vie privée notamment, l'Europe annonce, ne serait-ce que dans le titre du RGPD, l'une des finalités de son mandat dans ce domaine : celui de la protection des personnes.

Mais il faut relever que jamais un texte européen n'avait fait l'objet d'autant de pressions de la part de lobbies. C'est donc un texte de compromis qui a été adopté et a aussi pour objectif la libre circulation des données, comme celle des autres marchandises, au sein du marché unique.

Quelles sont les protections qu'il institue ? L'une d'elles est déjà de nous informer de ce que font de nos données les opérateurs, dits « responsables de traitements ».

A cet égard — et de bien d'autres puisque l'essentiel des protections figurant dans le RGPD existait déjà dans la loi Informatique et libertés de 1978 —, ce n'est pas une nouveauté. Mais ce qui l'est davantage tient aux sanctions des manquements : elles sont sans commune mesure. Jusqu'alors, les amendes infligées pouvaient être de 150 000 €, ou 300 000 € en cas de récidive (3 millions depuis 2016). Maintenant, il est possible de d'infliger des sanctions de 20 millions d'euros et jusqu'à 4 % du chiffre d'affaires mondial (soit environ 11 à 20 milliards d'euros pour Google). Sans compter la sanction réputationnelle pouvant se traduire par des désabonnements massifs.

Le RGPD maintient donc les exigences d'information, de recueil du consentement (mais le consentement n'est pas la seule justification possible d'un traitement de données), de traitement loyal, de sécurisation, et réaffirme les droits des personnes qui figuraient déjà dans la loi française et la précédente directive européenne : d'accès à leurs données, de rectification et d'opposition, voire de demander l'effacement.

Mais il en pose aussi de nouveaux : par exemple le droit à la portabilité des données, c'est-à-dire de transporter son « sac de données » quand on change d'opérateur, chaque citoyen

ayant ainsi la possibilité de reprendre la maîtrise de ses données. D'ailleurs, ce droit participe d'un principe plus large, celui d' « autonomie informationnelle », qui pourrait émerger au niveau constitutionnel, comme pour l'environnement.

Pour autant, pour que tout ce système fonctionne, il faut que les citoyens s'emparent de ces droits, comme ils y sont invités en matière d'environnement ou de cultures biologiques.

Or, cela se heurte à deux paradoxes :

- le "privacy paradox" qui consiste à prétendre que l'on est attaché à la protection de sa vie privée mais, en même temps, à l'exposer à longueur de journée ;
- celui de la gratuité : tous ces services semblent gratuits. Or, l'invitée rappelle un mantra de l'économie numérique : « Quand c'est gratuit, c'est vous le produit » On accepte la gratuité, sans se rendre compte que la monnaie d'échange est l'accès à nos données personnelles. Et il est très difficile de revenir en arrière.

Le tout fait que le consentement est très difficile à refuser, lorsque l'on met en balance un certain nombre de services, tout à fait exceptionnels, qui semblent gratuits.

Débat :

Q. Comment réagissent les Américains, face à ce règlement qui concerne quelques-unes de leurs grandes sociétés ? Ils ont coutume de penser que ce qui est bon pour l'Amérique est bon pour le monde. Alors, comment peut-on leur imposer les contraintes du nouveau règlement ?

Il faut bien avoir à l'esprit que les GAFA[2] sont américains, mais que leur marché est européen. Les 500 millions d'Européens sont leurs pourvoyeurs de données, et ils ne peuvent pas s'en passer.

Du coup, c'est vrai que ce règlement a été un coup de tonnerre pour les Américains. Mais il faut aussi se souvenir que, pendant qu'il était encore en discussion et que de gros blocages l'empêchaient d'avancer, Google a été contraint de mettre en œuvre de façon effective et opérationnelle le « droit à l'oubli », en raison d'une décision de la Cour de Justice de l'Union. Celle-ci a alors fait apparaître la nécessité d'un texte. En effet, un citoyen espagnol, Mario Costeja Gonzàles, avait intenté une action pour faire valoir ce droit, car des ennuis financiers que lui et sa femme avaient eus douze ans auparavant ressortaient systématiquement quand on recherchait son nom sur Google. Google a fait valoir qu'il ne faisait que répercuter des informations parues dans un journal, mais qu'il n'avait pas créé cette information. Le Cnil espagnole a donné en partie raison à M. Gonzàles, puis la Cour de justice européenne (CJUE) a demandé à Google d'enlever des résultats de recherche — déréférencer — pouvant nuire à la personne et dont l'utilité n'était plus avérée. Il s'agissait d'une interprétation très extensive du droit européen existant.

De son côté et à la suite de cette décision, la Cnil française a reçu beaucoup de demandes de déréférencements. Elle a même estimé que ce droit à l'oubli devait s'étendre à l'ensemble

[2] GAFA : acronyme pour désigner les grandes entreprises traitant des données personnelles, dont les plus emblématiques sont Google, Apple, Facebook, Amazon.

du monde (à toutes les extensions du moteur de recherche), pas seulement à la France, ce que Google conteste encore aujourd'hui.

Précisions que le règlement européen définit quant à lui son propre champ d'application : il s'applique non seulement quand un opérateur a son siège social ou son lieu de traitement dans un pays de l'UE, mais aussi dès qu'un opérateur offre des biens ou des services à des citoyens européens, ou dès qu'il cible des comportements de personnes qui résident en Europe.

On est donc dans un domaine où l'Europe se montre forte. Elle a tapé du poing sur la table, notamment par l'intermédiaire de sa Cour de Justice, à un moment où tout semblait bloqué.

Q. Quid de la propriété des données ?

C'est une idée que récuse l'invitée. Les données ne sont pas, selon elle, des marchandises, mais des éléments de la personnalité, du comportement. La valeur d'une donnée individuelle est insignifiante. Elle ne devient valorisable qu'en relation avec les autres. La CJUE s'est d'ailleurs fondée sur l'article 8 de la Charte des droits fondamentaux, c'est-à-dire sur la reconnaissance d'un droit fondamental des personnes à la protection des données et non pas sur un droit de propriété ou un quelconque retour de valeur.

Q. La directive européenne de 1995 portait une ambiguïté, car l'Europe n'avait de compétences qu'en matière économique et on est passé par ce biais pour construire une directive portant sur la libre circulation des données. En quoi le règlement de 2016 change-t-il quelque chose ?

La règlement porte le même nom : « Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » Mais le changement par rapport à la directive de 1995 est lié à l'activation en 2014, par la CJUE, d'un droit fondamental des personnes à la protection de leurs données. Le compromis est toujours à l'œuvre : c'est une marchandise qui doit circuler librement, mais au bout, il y a une personne qu'il faut protéger.

Q. Le fait que le consentement permettrait de se dispenser de payer certains services ne rétablit-il pas la notion de valeur marchande pour les données personnelles : échange de données contre prestation d'un service ?

Ce paradoxe fait aujourd'hui l'objet d'une discussion en Europe, autour du projet d'un autre texte, une directive qui porterait sur les contenus numériques, pour faciliter et réglementer l'accès à ces contenus (services, objets connectés). Le texte reconnaîtrait que l'accès à ces services pourrait se faire soit par un paiement monétaire, soit par la fourniture de données personnelles. Il constaterait donc qu'il y a échange, valorisation monétaire des données. Mais il n'a pas été adopté et a fait l'objet d'une forte contradiction, précisément pour son risque de contradiction avec le RGPD. On s'en est sorti en disant que ce n'est pas parce que c'est un élément de la personnalité qu'il ne peut pas y avoir un consentement pour laisser un usage. Par exemple l'usage de l'image ou du nom d'une personne peut être monnayé, c'est déjà le cas. Cela ne correspond pas pour autant à la propriété d'un bien.

Q. L'intérêt des données individuelles change au cours du temps. Elles ont une durée de vie. Comment traite-t-on leur obsolescence ?

Dans tous les textes — loi de 1978, directive de 1995 et règlement de 2016 — il est dit qu'on n'a le droit de conserver les données que pour la durée nécessaire à la finalité exprimée au moment où ces données ont été collectées.

C'est une question compliquée… L'ambiance est au Big Data, c'est-à-dire à conserver les données « à tout hasard » pour une réutilisation ultérieure, que l'on n'imagine pas aujourd'hui. Mais les textes ne le permettent pas.

Cependant, effectivement, ce n'est pas si grave, car les données deviennent vite obsolètes (déménagement, changement de nom, de profession…). Pour le cas de M. Costeja, évoqué précédemment, les données avaient douze ans, mais pouvaient continuer de nuire à sa réputation. Dans ce cas, on n'a pas touché à l'existence de l'information — l'article de journal reprenant ses déboires n'a pas fait l'objet d'un effacement — mais à sa visibilité : on a « seulement » bloqué sa reprise dans les résultats d'un moteur de recherche.

Q. Comment les Gafa peuvent-ils distinguer les résidents des non-résidents ?

Premier critère : est-ce que la plateforme offre des services à des Européens ? Ça se voit assez facilement. Deuxièmement, ils savent tout de nous par la géolocalisation, notre adresse IP, nos recherches, par les sites qui sont en français… Ça n'est vraiment pas difficile à savoir pour eux !...

Q. Il est parfois utile et nécessaire de faire un usage collectif des données individuelles. Comment peut-on rendre cet usage compatible avec le RGPD ?

Il n'est pas interdit de faire un usage des données individuelles pour un usage d'intérêt commun. D'abord, on peut anonymiser les données. C'est extrêmement difficile à faire, mais si on y arrive, on sort du règlement. Les données ainsi anonymisées peuvent être utilisées à des fins statistiques ou de recherche, par exemple. Par ailleurs il est bien entendu possible d'utiliser les données personnelles pour un usage public : il est évidemment nécessaire par exemple d'avoir le nom et le prénom et d'autres renseignements pour les documents d'identité.

Pour autant, les pouvoirs publics sont sous le regard de l'Europe et du droit européen. Ainsi, l'Irlande était visée par un arrêt de la Cour de Justice de l'UE de 2014, car elle demandait, pour ses documents d'identité, des empreintes biométriques considérées comme beaucoup trop nombreuses ; elle les conservait longtemps. La CJUE a considéré que c'était disproportionné.

En France, on a eu des débats du même genre avec le fichier des titres électroniques sécurisés (fichier TES) qui centralise beaucoup d'éléments, y compris biométriques, de la population française dans un fichier central. Or, la France est très sensible à l'usage des données dans des fichiers publics (c'est la raison pour laquelle la loi Informatique et libertés de 1978 a été votée et l'une des premières au monde) : fichiers des juifs en 1942, projet Safari… Il y a des aspects très culturels aux réactions de la population.

Il est vrai qu'aujourd'hui nous sommes dans un contexte où, avec la menace terroriste, le curseur n'est plus placé au même endroit.

Q. Qu'est-ce que le RGPD change pour les Gafa, par rapport à la loi de 1978 ?

Pour les entreprises, c'est le branle-bas de combat. La mise en conformité leur coûte cher en formation, en changements de procédures, et mise en place de réponses à la portabilité, etc. Ce pan du droit, qui existait déjà à 80 % depuis 1978, était considéré comme sympathique, un peu inoffensif, mais pas trop contraignant. Maintenant, c'est la course à la conformité — pour les plus zélées — car les sanctions sont très lourdes, même si elles ne vont pas tomber du jour au lendemain.

Pour les entreprises, c'est la même prise de conscience que pour les citoyens. Malheureusement, ce droit est extrêmement complexe, alors même que c'est un enjeu démocratique fondamental.

Q. Les données de santé sont insuffisamment utilisées. La protection des données individuelles met un frein à l'utilisation collective qui pourrait en être faite dans une finalité d'intérêt général. On est dans un système trop protecteur, qui freine l'innovation.

Les biens communs doivent évidemment être préservés. En particulier les données de santé ont une « valeur » non monétaire pour l'ensemble de la société, notamment quand on les met en relation avec d'autres.

Des réponses viennent des malades eux-mêmes : certains malades ont décidé de mettre en commun les données les concernant, pour s'en assurer la maîtrise. Ce n'est qu'une partie de la réponse, mais elle est insuffisamment explorée.

On peut en effet estimer que la protection des données individuelles fait que l'on innove moins.

Mais le RGPD met en place un changement de philosophie, sous la forme de la responsabilisation des acteurs. L'idée pourrait formulée ainsi : « Vous faites ce que vous voulez, mais prenez des garanties lorsque vous faites des choses dangereuses : faites une étude d'impact, analysez vos risques… Et si ça n'est pas suffisamment équilibré, on viendra vous dire que ça ne va pas » Auparavant, on faisait les formalités auprès de la Cnil, et quand l'accord était obtenu, on n'y pensait plus.

Mais il est sûr qu'en matière de données de santé, on est en passe de prendre du retard par rapport à toute la masse de données qui a été accumulée par ailleurs.

Q. Il est pratiquement toujours impossible de vérifier qu'une donnée est anonymisée.

Effectivement, une recherche récente d'Oxford montre que 95 % des données qui étaient censées être anonymisées ne l'étaient pas en réalité. Il s'agissait de données de géolocalisation. Il devient de plus en plus difficile de ne pas remonter à la personne à mesure que les données s'accumulent et permettent de plus en plus de croisements.

Q. Les données perdent certainement de l'intérêt avec les années pour l'individu auquel elles se rapportent. Mais elles gardent un intérêt de type public pour la société. Si on impose l'effacement, on se prive de cette utilité collective.

Effacer des informations c'est effectivement effectuer une sorte de privatisation de nos données publiques, de nos archives, de notre mémoire collective.

Le problème est que rien ne s'oublie plus, alors qu'auparavant, il existait une sorte d'oubli social. D'où la nécessité d'un compromis entre les deux impératifs. Le RGPD reprend donc les exceptions « sociales » qui existaient antérieurement : conservation pour des nécessités d'archives, statistiques, d'information, de recherche.

Un débat est très important actuellement relativement aux décisions de justice : elles doivent être rendues publiques et mises en large accès (open data), mais il est nécessaire de les anonymiser (ce qui n'est pas toujours possible, quand par exemple une personne est reconnaissable aux faits relatés).

Q. Lorsque l'on parle d'effacement, qu'est-ce qui garantit qu'elles ont disparu ? Une copie peut toujours subsister quelque part. En particulier, comment s'assurer que la conservation ne se fait pas hors du territoire ?

L'effectivité du droit est une question très générale. On peut quand même penser à l'effectivité de la sanction. On l'a vu avec le droit de la concurrence : Microsoft ne le respectait pas. Quand la menace de sanction s'est chiffrée en milliards d'euros, la société est rentrée dans le rang.

Sur ce sujet, la Cnil a acquis plus de pouvoir avec la nouvelle loi.

Q. Y a-t-il des mesures qui auraient dû selon vous figurer dans le règlement, et qui ne s'y trouvent pas ?

Suite à un intense lobbying, le droit « à l'oubli » — plus exactement le droit de demander un déréférencement à un moteur de recherche si une information est gênante pour la réputation ou la vie privée — ne figure finalement pas dans le texte en tant que tel. En conséquence, ce droit, introduit en 2014 par la CJUE, c'est-à-dire une instance non démocratique et sous forme d'une sorte de « putsch » judiciaire, reste purement judiciaire, non législatif.

Q. Y a-t-il un suivi de ce qui se passe en Chine ?

La Chine est un monde en soi du point de vue numérique, qui soulève notamment la question de la neutralité du Net. Cette question se pose aussi aux États-Unis, et cela nous impacte directement.

En Chine se met aussi en place une société de la surveillance et de l'évaluation généralisée, d'une reconnaissance faciale, même de dos, etc. C'est un choix politique… Il faut tenir compte de la culture de chaque société, y compris avec l'Allemagne, les États-Unis (culte de la liberté d'expression et de la liberté d'entreprise).

La relation avec la Chine ne pourra pas se faire de la même manière qu'avec les Gafa (pour ces derniers, nous sommes leur marché, ils ne peuvent pas le contourner ; le marché chinois est quant à lui très important). Néanmoins, les BAXT (leur GAFA), s'ils veulent s'implanter en Europe, seront obligés de suivre les règles européennes (Alibaba est déjà implanté par exemple).

Q. Comment assure-t-on la protection des mineurs ?

Cela a donné lieu à une querelle franco-française. Le règlement européen laissait une marge d'interprétation aux États sur certains points, dont celui de l'âge de la majorité numérique. Le Sénat et l'Assemblée nationale se sont déchirés pendant des semaines pour savoir s'il fallait retenir 15 ans ou 16 ans (l'Irlande a retenu 13 ans). On a finalement retenu 15 ans, pour s'aligner sur la majorité sexuelle.

Cette disposition est difficile à mettre en œuvre, car le jeune déclare ce qu'il veut. Mais certains parlementaires jugeaient important qu'un seuil soit fixé par la loi. Les opérateurs doivent donc mettre en place une procédure de vérification. Il existe par ailleurs des sociétés d'éducation au numérique.

Quant aux addictions possibles, on a l'exemple de l'addiction au jeu en ligne : il existe une obligation, pour les opérateurs, de transmettre aux autorités publiques les données qui pourraient traduire un risque d'addiction.

Q. Comment se gère le droit à l'oubli pour des personnes publiques, tels que les hommes politiques ? Leurs déclarations ou actions font partie d'un patrimoine commun.

Il y a une dizaine de critères pour juger du droit à l'oubli. Parmi les plus importants, on trouve la notoriété de la personne et son caractère public, ainsi que la participation des données à un débat d'intérêt général.

Q. Vous avez parlé d'une autre directive en préparation. Pouvez-vous nous en dire plus ?

Il y a actuellement une salve ininterrompue de textes : une loi nationale du 20 juin 2018 a été votée pour articuler le droit français et le règlement mais il sera finalement difficile de savoir, pour un cas particulier, quand le règlement ou la loi s'appliquera. Suivront normalement une ordonnance pour cette articulation (pour dire quand l'un ou l'autre doit s'appliquer, voire pour corriger les erreurs). Le Conseil constitutionnel a dit, ce qui est surprenant, qu'il n'y avait aucun problème d'accessibilité au droit pour le citoyen…

On attend également certains textes qui viendront peut-être parfois contredire le RGPD. Un règlement européen « e-privacy » doit être adopté, plus précis car concernant les communications électroniques et les cookies. Ce texte est difficile à adopter car il n'est pas consensuel. Il pourrait en partie détricoter ce qui a été fait par le RGPD.

Un autre texte, qui s'appelle « Free Flow of Data » concernerait les données non personnelles, par exemple rattachées à une machine. Mais avec la diffusion des objets connectés, on se rapprochera de plus en plus des données personnelles.

Q. Comment peut-on expliquer que, dans la préparation du règlement, après quatre années de luttes acharnées, on soit arrivé à un consensus ?

Il n'y avait aucun consensus, ni entre les États, ni entre les acteurs. Ce fut une lutte impitoyable. Le rôle de la CJUE fut très important puisqu'elle a montré que, en l'absence de consensus sur un texte (les discussions étaient bloquées), elle n'hésiterait pas à imposer des solutions très protectrices (le fameux droit « à l'oubli »). Peut-être les pays se sont-ils rendu également compte que, par manque ou moins de références historiques sur ce sujet, l'enjeu était moins national qu'européen ? Que « l'ennemi » commun était suffisamment puissant pour coaliser les européens sur un compromis ?

On peut penser que la CJUE continuera à avoir une position très personnaliste.

Il y a eu un sursaut des valeurs européennes dans ce domaine.

Q. Comment harmoniser la position des différentes « Cnil » nationales ?

Il est difficile de préjuger de ce que feront les « Cnil » hollandaise, française ou estonienne. Il y a cependant le système du guichet unique, qui devrait avoir une influence : une des « Cnil » prendra la main et collaborera avec les autres, pour peu qu'il y ait plusieurs États impactés. On devrait ainsi arriver à terme à des solutions d'interprétation qui seront homogènes.

Un participant au groupe de travail de préparation du RGPD confirme que l'on a passé six à huit mois sur le seul point du guichet unique. Et les gouvernements s'en sont remis in fine à cette solution. Un point dur a été aussi l'exception sur les archives.

Q. Que penser des réactions citoyennes contre le compteur Linky ?

Elles témoignent d'une montée en puissance des préoccupations citoyennes à l'égard des données, ce qui est une bonne chose. Il faut à ce sujet souligner l'ouverture faite par la loi de 2016 sur la « justice du XXI^{e} siècle » : elle offre la possibilité de mener des actions de groupe ; elle a été actualisée par la loi du 20 juin 2018 pour les données.

D'ailleurs, le lendemain de la mise en application du RGPD, c'est-à-dire le 26 mai 2018, des actions de groupe contre certains Gafa ont été lancés par l'association « La quadrature du net », pour manque de transparence de Facebook et autres manquements supposés au règlement, ainsi que d'autres en Europe.

Q. Vous avez souligné la lourdeur des sanctions. Pensez-vous qu'elles seront appliquées ? En effet, certains citoyens sont très attachés à des services.

On est là dans une des inconnues de ce texte : va-t-il être appliqué ? Les sanctions seront-elles mises en œuvre ? Ou leur aspect dissuasif sera-t-il suffisamment fort pour qu'il n'y ait pas besoin de les appliquer ?

Inversement, aux États-Unis, certains se posent la question « Ne faut-il pas nationaliser ces quasi-services publics ? » On est dans l'inversion des cultures !...

D'un côté, on ne voit pas pourquoi la CJUE changerait de position et ne pousserait pas à l'application des sanctions. De son côté, la Cnil française a fait savoir publiquement que le temps d'adaptation (à la loi de 1978 !) était terminé.

Q. N'y a-t-il pas un risque d'une segmentation du monde, à un horizon de dix ou vingt ans, avec les systèmes européen, chinois, américain ou autre… ?

Là, on dévie de la question des données à celle de la neutralité du Net. Reste-t-on avec l'idée qu'internet est un bien public mondial, même si certains s'en sont exclus (Russie, Chine), ou remet-on en cause cette idée, en faisant par exemple payer davantage certains que d'autres, etc., ce qui revient à privilégier certains contenus sur d'autres ? Accepte-t-on de faire des différences dans le contenu qui transite sur le Net en fonction de divers critères ?

Nous sommes au milieu du gué, et tout peut basculer d'un moment à l'autre. C'est absolument décisif. Les États-Unis ont pour l'instant basculé dans un sens — la fin de la neutralité (mais il y a des réactions) — tandis que l'Europe tient bon pour l'heure.

Q. Que peut-on dire sur les algorithmes ?

Cette question est présente dans le règlement et dans la loi Informatique et libertés. La question est de savoir si, à terme, des algorithmes vont prendre des décisions sur nous, et le faire sans intervention humaine. Or le règlement proclame un droit de ne pas subir une décision juridique ou une décision qui a des effets significatifs et qui serait totalement automatisée. Des exceptions sont possibles, certes : si la personne y a consenti, si c'est nécessaire pour la conclusion ou l'exécution d'un contrat, ou encore si un État décide qu'il reconnaît certains cas. La France s'est engouffrée dans cette dernière exception pour les décisions de l'Administration : elles peuvent être automatisées. L'une des illustrations est « Admission post-bac » (APB), devenu cette année « Parcours Sup ».

Dans ce cas, la loi a introduit certaines garanties, qui ont été réinterprétées par le Conseil constitutionnel : il faut dire à la personne que son cas est traité par un algorithme, annoncer les critères du paramétrage, permettre d'accéder à ce que l'algorithme a fait, pouvoir le contester.

Reste la question de savoir si l'on impose que l'algorithme soit vérifiable et soit expliqué. Pour les algorithmes publics, ils sont soumis, comme les autres documents publics, à l'ouverture de leur code source.

Notons que la question se posait déjà depuis longtemps. Le public donne l'exemple des radars automatiques enregistrant dix mille excès de vitesse, qu'un magistrat va, d'un seul paraphe, valider. Il ne les a évidemment pas constatés individuellement. Cette disposition est donc quelque peu décorative, voire hypocrite.

L'évolution à prendre en compte tient aux algorithmes qui pratiquent l'auto-apprentissage : ils créent des règles de décision, dont personne, même *a posteriori,* ne peut expliciter les critères.

Pour le jeu de Go, des machines ont procédé de façon incompréhensible et fini par battre les meilleurs joueurs.

C’est pour cela que l’on impose, pour les algorithmes de l’Administration, que leur concepteur conserve sur eux la maîtrise. On aura des difficultés en face d’algorithmes plus autonomes…

Q. Facebook a clairement admis devant le Sénat américain et devant le Parlement européen qu’il n’avait pas respecté les règles. Il s’est fait taper sur les doigts, mais on n’a pas entendu de sanctions sur ce sujet. N’est-ce pas un mauvais signal ?

La justice ne va pas aussi vite que Facebook. Il y a des actions en cours aux États-Unis et en Angleterre. Les sanctions viendront, mais plus tard.

Q. Que penser du Dark Web ?

Il y a de tout dans le Dark web! Du bon — des moyens de communiquer pour des défenseurs de la liberté d’expression — et du moins recommandable — des trafics illégaux de tous types. C’est un monde en soi. C’est caché, mais cela ne veut pas dire que tout soit condamnable… Mais on a évidemment des difficultés supplémentaires pour assurer une régulation de ce monde…